

A photograph showing a group of people from the chest down, wearing blue long-sleeved shirts. They are all holding a thick, light-colored, coiled rope or cable. The rope is held in a way that it forms a continuous line across the frame, with each person's hands visible gripping it. The background is slightly blurred, focusing attention on the hands and the rope. The overall tone is professional and collaborative.

THE POWER OF TEAM:

THE MAKING OF A CIO

DAN PORTER - ALEX BENNET - RON TURNER - DAVE WENNERGREN

The Power of Team: The Making of a CIO

To all the professional men and women—uniformed, civilian, and contractor—who contribute to keeping the United States Navy and Marine Corps team the greatest in the world.



The value of information technology initiatives is found in transformation of core business functions and processes. Exceptional initiatives produce exceptional results.

—Dan E. Porter, Chief Information Officer

Our knowledge management efforts of today are contingency planning for tomorrow. It's a brave new world!

—Alex Bennet, Deputy Chief Information Officer,
Enterprise Integration



I like to refer to the IS&T area products as the critical underpinnings required for the health and growth of the IT economy across the Department.

—Ron Turner, Deputy Chief Information Officer,
Infrastructure, Systems and Technology

The measure of an effective CIO is the ability to successfully lead change.

—David M. Wennergren, Deputy Chief Information Officer,
eBusiness and Security



Table of Contents

A Message from the DON CIO	9
Acknowledgements	11
Introduction	13

CHARTING THE COURSE

CHAPTER 1	The Congressional Mandate	15
	The Goldwater-Nichols Act	15
	The Paperwork Reduction Act	16
	The Clinger-Cohen Act	17
	The Government Information Security Reform Act (GISRA)	19

CHAPTER 2	Thinking Strategically	25
	The Vision	26
	The Strategic Plan	28
	The CIO Organization	31
	DON CIO Critical Success Factors	35
	Collaborating with Out-of-the-Box Thinkers	38
	Concluding Thoughts	44

CHAPTER 3	Connecting Across the Enterprise	45
	Teams and Communities	45
	Event Intermediation	47
	Forums	47
	Awards	48
	Communications and Outreach	52
	Concluding Thoughts	56

THE INITIATIVES

CHAPTER 4	Focus on Governance and Infrastructure	57
	Introduction	57
	4.1 IT Oversight	64
	4.2 IT Governance	70
	4.3 IT Standards	75
	4.4 IT Infrastructure Architecture	78
	4.5 Navy Marine Corps Intranet	81
	4.6 IT Enterprise Architecture	90
	4.7 Data Management	96
	4.8 Electromagnetic Spectrum	99

	4.9 Technology Enablement Strategies	108
CHAPTER 5	Focus on eGovernment	117
	Introduction	117
	5.1 eBusiness	121
	5.2 Knowledge Management	128
	5.3 Naval Libraries and Information Services	141
	5.4 Enterprise Portal	147
	5.5 Knowledge Taxonomy	152
	5.6 Smart Card	163
	5.7 Records Management	171
CHAPTER 6	Focus on People	177
	Introduction	177
	6.1 IM/IT Workforce Competency Management	180
	6.2 Integrative Competencies	189
	6.3 Information Literacy	195
	6.4 Organizational eLearning	201
	6.5 Communities of Practice	206
	6.6 Section 508	211
CHAPTER 7	Focus on Security	215
	Introduction	215
	7.1 Y2K	218
	7.2 Information Assurance	222
	7.3 Critical Infrastructure Protection	228
	7.4 Privacy	239
CHAPTER 8	Focus on Dollars	247
	Introduction	247
	8.1 The IT Capital Planning Process	249
	8.2 Investment Management	261
	8.3 Enterprise Licensing	267
	8.4 Metrics	272
	FULL SPEED AHEAD	
CHAPTER 9	Managing Change	283
CHAPTER 10	The Future and the CIO	301

APPENDICES

Acronym List	309
Glossary	317
Index	339
References	345

A Message from the DON CIO

It wasn't out of aggrandizement. Have you ever found yourself wondering about an author's motivation? Many do it because it's their job; others for the money; some for fame. We didn't undertake the writing of this book for any of those reasons.

As the Acquisition Reform Executive back in 1995, my three staff members and I were in the midst of "imagineering" a new type of facility where teamwork and collaboration could be learned and practiced, and subjected to scientific inquiry. One of the key concepts which would be embodied in that "collaborating" was systems thinking. We journeyed to Massachusetts Institute of Technology to visit Dr. Jay Forester, the father of systems thinking, to seek his views and learn from his decades of experience. After we had finished painting our thought picture of how this center would be designed, and our vision for breaking down organizational, functional and geographical boundaries, we anxiously awaited his reaction. He thought for a moment or two, and then said, "What makes you think people want to share?" We were somewhat shaken by that question, and you could say that the four of us have been trying to answer that question ever since.

Sharing. Is it an attitude? A behavior? A cultural attribute? An outcome shaped by incentives? Maybe all of these things? We have made it a core value in the Department of the Navy (DON) Acquisition Reform Office and the Chief Information Office. This core value of sharing has been integral to the success DON has enjoyed in pioneering concepts of knowledge management, and motivates us in our production of tools and guides.

We produced this book because we wanted to share our experiences and insights as we constructed and implemented an agenda for the Chief Information Office. What's the catch? There isn't one. We aren't trying to sell anything. We know that we have a lot to learn and miles to cover in our continuous improvement journey, but we also know we've learned a lot along the way. Enjoy the book. Pass it along to a friend or colleague. Feel free to use anything you find useful. Contact us to let us know what you think. Share.

A handwritten signature in black ink, appearing to read "D. E. Porter". The signature is fluid and cursive, with a large initial "D" and "E".

D. E. Porter

Acknowledgements

The making of the Department of the Navy Chief Information Officer (DON CIO)—as well as the making of this book—was a true collaborative effort involving many people. Without their significant contributions, the DON CIO would not function as effectively as it does, and this book certainly would not exist.

Early champions who recognized the transformational potential of information technology in the DON were Vice Admiral Art Cebrowski, the founding father of Network Centric Warfare, and Admiral Archie Clemins, who put information theory into practice every day in the Fleet.

At the top of the list are the early leaders of the CIO team, Dr. Marv Langston and Dr. Ann Miller, and the many members of the DON CIO Team—an extraordinary group of hardworking and dedicated people who have effectively carried out the strategic vision of the DON CIO. They include Mr. Dan Porter, the current DON CIO, and his three deputy CIOs—Ms. Alex Bennet, Mr. Ron Turner, and Mr. Dave Wennergren.

Members of the team, past and present, who have helped make the DON CIO a success are Tom Albright, Bob Alderman, Lieutenant Commander Emory Anderson, Lieutenant Colonel Greg Andrews, Bruce Anich, Pauline Armstrong, Scott Badger, Brian Baker, John Baldwin, Jane Barkley, John Barron, Charley Barth, Ramon Barquin, Jim Bates, Miriam Bayley, Dave Bennet, Betty Bland, Wes Blankinship, Carl Bolter, Joe Broghamer, Adrienne Brown, Steve Bury, Al Bush, Lee Canterbury, David Carder, Castina Carey, Rob Carey, Steve Carey, Geno Celia, Hank Chase, Dale Christensen, Pat Christensen, Tony Cieri, Commander Kimberly Coffey, Jim Collins, Christina Cooksey, Captain Cray Coppins, Brian Cowan, Alan Craig, Linda Lou Crosby, Brooke Crouter, Karen Danis, Howard Davey, Carl Day, Mahnaz Dean, LaRae Dudley, Lieutenant Commander Eric Elser, Dan Elwell, Commander Gary Evans, Patrice Feemster, Pat Fontaine, Roderick French, Robert Fuentes, Richard Gallagher, Patsy Gates, Commander Lynn Gaudreau, Kelli Gillis, Karen Gleason, Robert Green, Jeff Greene, Floyd Groce, and Charles Gunn.

Also part of the team are Jennifer Harper, Matthew Hart, Jack Hawxhurst, Maggie Hiser, Colleen Herrmann, Linda Hidalgo, Freda Higdon, Barbara Hoffman, Captain Peter Hyers, Theresa Jackson, Michael Jacobs, Rick Johnson, Bob Jones, Brenda Jones, Frank Jones, Laurie Jones, Penny Jones, Yvonne Jordan, Captain James Kantner, Scott Kellen, Angela Keys, Hun Kim, Bob Knetl, Jim Knox, David Layton, Captain Mike LeValley, Debbie Lemmeyer, Joeneicy Lewis, Robert Lewis, Adam Lough, John Lussier, Richard Lynch, Dan Mannerino, Ward Masden, Judy McCarthy, Captain Sheila McCoy, Hugh McCullom, Captain John McDivitt, Commander Jim McDonough, Captain James “Spuds” McKenzie, Commander Andy Meldrum, and Lisa Metzke.

The team also includes Michael Minogue, Bryan Morton, Commander Joe Murphy, Indira Nair, Delpha Nichols, Rebecca Nielson, Janey Nodeen, Kevin O’Leary, Elizabeth Olson, SK2 David Pacheco, Harry Palm, Ken Phannavong, Jean Pate, Captain Jerry Peeters, Jennifer Picha,

Lynda Pierce, Kim Plyler, Neil Pollack, Mary Purdy, Penny Rabinkoff, Erv Raines, Connie Reid, Don Reiter, Rich Rhoadarmer, Darwin Roberts, Kealy Roderer, George Rogers, Kris Roquemoore, Dave Rose, and Mel Rushing. Also, Josephine Schmidt, Edward Schmitz, Thomas Scruggs, Rachael Sedeen, Vince Serio, John Spann, Crystal Smith, Sandy Smith, Mark Smithburger, Frank Sowa, Kenya Spinks, Jim St. Clair, Dave Svec, Charles Swanson, Tom Swider, Crystal Symonette, Captain Cliff Szafran, Rick Therrian, John Tindal, Commander Katherine Tracy, Bob Turner, Emily Urban, John Verheul, Sharon Vermilyea, Commander Steve Vetter, Ginger Villanueva, NJ Villanueva, Robert Wagner, Mitch Waldman, Jim Wallen, Valerie Wallick, Dawn Walter, Steve Ward, Colonel Gary Washburn, Dennis Wells, Captain Mike Wendling, Ryan White, Tina White, Dave Whitney, Brian Wilczynski, Jon Wilham, Russell Williams, Joanne Wills, Craig Wilson, and Maggie Wilson.

Special acknowledgement to the editorial team, led by Lynda Pierce, Coordinator and Editor, and assisted by Delpha Nichols, Design and Layout, Rachael E. Sedeen, Dawn Walter and George Rogers, Graphics, and Ryan White, Cover Design.

In addition to the DON CIO team, numerous working groups, teams, communities of practice and communities of interest have contributed to making the DON Information Management/Information Technology (IM/IT) strategy a success. These include: the DoD Enterprise Software Initiative Working Group, eBusiness Stakeholders, Knowledge Management Community of Practice, Investment Practices Community of Interest, IM/IT Strategic Planning Working Group, the Knowledge-Centric Organization Project Team, the Y2K Virtual Town Hall Project Team, the cPort Project Team, the DON IT Investment Evaluation Process Product Team, the "Learning in a Virtual World" Project Team, the Information Literacy Project Team, the Knowledge Fair Project Teams, DON CIO Board of Representatives, Information Technology Standards Guidance Product Team, Information Technology Infrastructure Architecture Product Team, XML Working Group, Data Management and Interoperability Repository (DMIR) Product Team, DON Integrated Architecture Database (DIAD) Product Team and the Critical Infrastructure Protection Council and Working Group.

The DON CIO team also includes the Navy and Marine Corps, who lead implementation of DON policy and guidance across the Enterprise. And, finally, we must acknowledge the forward thinking of the Military and Civilian personnel who have embraced the new technology world and are determined to use the power of information and knowledge to make our country safe and secure!

Introduction

This book is intended to serve as a reference source for organizations that are charged with the responsibility of implementing information technology (IT), managing IT, or leading change in an IT organization. In this context, IT is used generically; it includes information management (IM) and knowledge management (KM). As you will see as you explore this book, IT is necessary, but not sufficient. To succeed, IT must be integrated with aggressive IM and KM programs.

There are three major sections in this book. The first Section—*Charting the Course*—includes Chapters 1 through 3. These chapters address the Congressional mandate for the Chief Information Officer (CIO) organization, the strategic thinking by Department of the Navy (DON) principals and partners, and how that thinking mapped out the strategy for building an effective organization; and how actively establishing and sustaining connections across the DON in the form of professional networks and relationships enabled the free flow of ideas. Included in Chapter 2 of this section is an explanation of the Critical Success Factors—the major characteristics and factors that have contributed to the success of the DON CIO. These Critical Success Factors are defined and associated with a related icon. These icons appear throughout the book where the specific Critical Success Factors have been important to the initiatives or areas being discussed. Also throughout the book you will find insights—nuggets of information or valuable lessons learned during the making of the organization.

The second Section—*The Initiatives*—includes Chapters 4 through 8. These chapters provide an in-depth look at the IT, IM, and KM initiatives important to the DON and, we believe, to any organization that uses technology to get its job done—virtually every modern organization in the world. These chapters are broadly grouped in the areas of Infrastructure, eGovernment, People, Security, and Dollars. The Initiatives section is one that you may want to read in bits and pieces, according to your interests. The introductions to each chapter provide detailed overviews. You may wish to delve deeper only into the specific areas that interest you. The Initiatives section can be used as a resource for the future, to draw upon when challenges emerge in specific areas, or to use as benchmarks for how a large government organization addressed these areas.

The third Section—*Full Speed Ahead*—includes Chapters 9 and 10. This section discusses the DON CIO change strategy, and shares specific thoughts and actions addressed toward achieving the cultural change so necessary for success. The closing chapter, “The Future and the CIO,” addresses the present and future environments, and looks at the future through the lens of Interoperability, Ubiquity, and Knowing.

To sum up, the short overview approach would be to read Chapters 1 through 3, the introductions to Chapters 4 through 8, and finish with Chapters 9 and 10. For an in-depth look at specific IT, IM, and KM initiatives, use the Table of Contents to pick and choose the topics that interest you, and read the appropriate sections within Chapters 4 through 8. Throughout the book there is repetition on key points to allow readers to understand the context of the material provided without reading the entire book. If you do read this book from cover to cover, please gloss over repeated material.

CHAPTER 1

The Congressional Mandate

In recent years, Congress has acted decisively on several fronts to provide the legislative foundation for the creation of effective Federal Chief Information Officers that are the single focal points for information management within their agencies. Significant legislation in this area includes the Goldwater-Nichols Act, the Paperwork Reduction Act, the Clinger-Cohen Act, and the Government Information Security Reform Act (GISRA). A short discussion of the substance of these Acts and their impact on the DON is included below.

THE GOLDWATER-NICHOLS ACT

The Goldwater-Nichols Department of Defense Reorganization Act of 1986 generated the first major defense reorganization since the National Security Act of 1947. The Goldwater-Nichols Act strengthened Military operational authority through the Chairman of the Joint Chiefs and designated the Chairman as the principal Military advisor to the President, National Security Council, and Secretary of Defense. Department of Defense (DoD) focus on joint operations is largely born from the changes directed by the Goldwater-Nichols Act.

Another important aspect of Goldwater-Nichols is the delineation of functions that must be carried out by the Secretaries of the Military Departments. The Act specifically instructed the Secretary of the Navy to establish an office/entity within the Office of the Secretariat to conduct information management. The term “information management” is neither defined in the statute nor discussed in legislative history. However, the term has been broadly defined in DoD Directive 8000.1, “Defense Information Management (IM) Program,” dated February 2002. The term includes “information resources management,” which is defined later in the Paperwork Reduction Act and the Clinger-Cohen Act as the “process of managing information resources to accomplish agency missions and to improve agency performance” [44 U.S.C. 3502(7); Section 5002 (4) of Clinger-Cohen]. The term “information management” is also defined in OMB Circular A-130 “Management of Federal Information Resources” as meaning the “planning, budgeting, manipulating, and controlling of information throughout its life cycle.”

In addition to assigning to the Secretariat, responsibility for the function of information management, Goldwater-Nichols specifically indicates that “no office may be established or designated within the Office of Chief of Naval Operations (CNO) or Headquarters, Marine Corps (HQMC), to conduct the information management function” [10 U.S.C. Section 5014 (C) (2)]. Legislative history indicates that the language “no office” was selected with care. The Conference Report indicates the intent is that no office within the Military headquarters staff may be established or designated to perform any of the listed functions on a permanent basis. Goldwater-Nichols further provides that the responsible Secretariat office is to provide the CNO and the Commandant of the Marine Corps the necessary staff support to perform their duties and responsibilities, thus avoiding

any unnecessary duplication of effort among the headquarters staffs [10 U.S.C. Section 5014 (c) (3)]. To further emphasize this point, 10 U.S.C. Section 5014 (e) requires the Secretary of the Navy to eliminate duplication of specific assigned functions among the Office of the Secretary, the Office of the CNO, and the HQMC.

THE PAPERWORK REDUCTION ACT

The Paperwork Reduction Act of 1995 changed many aspects of information collection by the Federal Government. The Act designated the Office of Management and Budget as the authority for “the use of information resources to improve the efficiency and effectiveness of governmental operations to serve agency missions.” The Act sought to minimize the paperwork burden placed on individuals, small businesses, educational and non-profit institutions. The Act set the goal of reducing information collections burdens imposed on the public by at least 10 percent during each of fiscal years 1996 and 1997, and 5 percent during each of fiscal years 1998, 1999, 2000, and 2001.

Under the Act, Federal agencies are specifically instructed to designate a senior official responsible for carrying out the agencies’ information resources management activities to improve agency productivity, efficiency, and effectiveness. The Act extensively details these responsibilities to include:

- Developing and maintaining a strategic information resources management (IRM) plan.
- Ensuring that information resource management operations and decisions are integrated with organizational planning, budget, financial management, human resources management, and program decisions.
- Maintaining current and complete inventory of the agency’s information resources.
- Conducting formal training programs to educate agency officials about IRM.
- Ensuring that the public has timely and equitable access to the agency’s public information.
- Implementing and enforcing records management policies and procedures.
- Implementing and enforcing policies, procedures, standards, and guidelines on privacy, confidentiality, security, and disclosure and sharing of information.
- Implementing and enforcing applicable government-wide and agency IT management policies, principles, standards, and guidelines.
- Promoting the use of IT by the agency to improve productivity and efficiency.
- Proposing changes in legislation, regulations, and agency procedure to improve IT practice.
- Assessing and managing risks of major information systems initiatives through a process that is integrated with budget, financial, and program management decisions, and used to select, control, and evaluate the results.

This Act laid the groundwork for the substantial changes in Information Technology legislated in the Clinger-Cohen Act.

THE CLINGER-COHEN ACT

In 1996 the Congress passed and the President signed the Information Technology Management Reform Act (ITMRA) and the Federal Acquisition Reform Act (FARA). Subsequently, in October 1996, these two divisions of the Defense Appropriations Act were officially named the Clinger-Cohen Act. This Act ushered in a new way of doing business in the Federal Government, helping to decentralize authority by providing greater latitude for managers to accomplish their missions, and enabling empowerment of field-level managers and headquarters commanders through increased delegations of authority. This landmark legislation positioned Federal Government acquisition of information technology (IT) at the forefront of Congressional oversight, and empowered the executive branch to establish an effective Federal IT infrastructure. The passage of the Clinger-Cohen Act gave recognition to the ever-increasing reliance on IT for management of many Federal Government functions, along with the requisite to acquire assets based on their capacity to enhance delivery of services.

The Clinger-Cohen Act was based upon proven, practical IT best practices used by leading organizations to improve performance and meet strategic goals. It is designed to help ensure that investments in IT provide measurable improvements in mission performance. The Act defines an integrated set of acquisition and management practices needed to build an effective IT infrastructure and refocuses IT management toward directly supporting missions.

The Clinger-Cohen Act represents a statutory response to historic inefficiencies in the procurement of IT resources. The 1994 “Computer Chaos” report, released by Senator William Cohen of Maine, brought to light some of the difficulties the Clinger-Cohen Act is intended to resolve, namely:

- Insufficient use of business processes in determining an appropriate investment strategy for IT.
- Prior IT investments made by Federal agencies that neither improved mission performance nor satisfied their original intent.
- Implementation of ineffective information systems resulting in waste, fraud, and abuse.
- Antiquated IT procurement strategies that did not adequately address the competitive and rapid life cycles market forces associated with industry IT products.

Specific highlights of the Clinger-Cohen Act that respond to this computer chaos include:

Repeal of the Brooks Act. The Clinger-Cohen Act repealed the 1965 Brooks Act, which was characterized by strict regulatory control over information resources management, an excessive documentation approval process, and a lengthy acquisition cycle. Decentralization of procurement authority means that the Department of the Navy can purchase its own IT without having to go through the General Services Administration. In removing the Federal Information Resources Management Regulation (FIRMR), the Act requires that simplified, clear, and understandable IT acquisition procedures be included in

the Federal Acquisition Regulation (FAR). It also mandates a shorter time (from 125 days to 100 days) for protest processing.

Establishment of Departmental Chief Information Officers (CIOs). The Clinger-Cohen Act established the CIO to replace the Senior IRM Official previously identified in the Paperwork Reduction Act. Rather than a Management Information System manager, who must focus on a fairly narrowly defined technical arena, the CIO must have a view of the whole organization and influence the direction of an organization. CIOs serve as the bridge between top executives, senior management, support staff, and IT professionals. They provide advice and assistance to the Head of the Agency, advise and educate all levels of management on the soundness of IT investment decisions, and participate in IT selection, deployment, and assessment of results. The DON CIO office was created in 1997 and remains committed to enabling process innovation and technology infusion to maintain a competitive edge in global security for the 21st Century.

Capital Planning. The Clinger-Cohen Act requires a process which provides for selection, control, and evaluation of IT investments. That process must be integrated with budget, financial, and program management decisions. Capital planning integrates agency strategic planning, performance measurement, and the budget process. One of the critical attributes of the capital planning process is that it links the mission, goals, and customers. The process also asks the questions of how well the organization's IT is achieving its original purpose; what its relative value, cost, and risks are today; and whether it should be continued, modified, or phased out. The DON Capital Planning Guide outlines the DON's capital planning policies and procedures and provides a model to assist command level managers in implementing an effective IT capital investment decision-making process.

Modular Contracting. The Clinger-Cohen Act supports modular contracting and suggests that a contract for a technology increment be awarded within 180 days, and vendors deliver system modules within eighteen months of contract award. Delivery, implementation, and testing of each technology increment will be independent of subsequent increment deliveries in the performance of principal functions. The agency's need for a system is satisfied in successive acquisitions of interoperable increments.

Business Process Reengineering. The Clinger-Cohen Act requires that reengineering be accomplished before an agency spends IT dollars, that the agency assess its IT investments to ensure accomplishment of the mission, and that agency processes be benchmarked with other like organizations in both government and industry.

Training and IT Workforce Competencies. The Clinger-Cohen Act requires quarterly assessment of IT skills requirements of personnel and an assessment of the agency's ability to match skills to employees. Success in IT management is people dependent. Training is essential at all levels to develop the new skills needed to acquire, evaluate, design, develop, integrate, and oversee highly complex information systems. Strategies to recruit, train, and retrain the best and the brightest must be designed and implemented.

Standards and Architectures. An enterprise architecture is critical to prevent fragmented, stovepiped systems. The CIO is responsible for the development of an integrated IT architecture that functions as an integrated framework for evolving or maintaining existing

IT and acquiring new IT to achieve the agency's strategic goals. The DON IT Standards Guidance and IT Infrastructure Architecture documents provided early guidance for applying IT in the DON, with a focus on interoperability and mission effectiveness.

Performance and Results Based Management. Agencies are required to establish strategic performance goals and assess performance progress against these goals. The assessment criteria include cost, schedule, productivity, and quality of results.

Strategic Planning. The Strategic Plan provides descriptions of operational processes, skills, and technology and the human capital, information, and other resources required to achieve strategic goals. IT investments should be aligned with the Strategic Plan.

THE GOVERNMENT INFORMATION SECURITY REFORM ACT (GISRA)

Consistent with the Paperwork Reduction Act and the Clinger-Cohen Act, the Government Information Security Reform Act of 2000 reconfirms the role of the Chief Information Officer as the provider of the agency's strategic view of architecture and cross-cutting security needs. Under GISRA the Department CIO is responsible for:

- Designating a senior information security official.
- Developing and maintaining an agency wide information security program.
- Ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques.
- Training and overseeing personnel for information security.

In order to fulfill GISRA requirements, agency CIOs must ensure that agency *security* programs fully integrate into the agency's enterprise architecture and capital planning and investment control processes. CIOs must work with agency program officials to ensure that the program officials understand and appropriately address risks, especially the increased risk resulting from interconnecting with other programs and systems over which the program officials have little or no control.

The legislation was in place, the mandate was clear, the task was daunting. The Department of the Navy forged ahead.

The Mandate for a CIO

The Secretary of the Navy shall establish or designate a single office within the Office of the Secretary of the Navy to conduct Information Management. No office or other entity may be established or designated within the Office of the Chief of Naval Operations or the Headquarters, Marine Corps, to conduct Information Management. (*Goldwater-Nichols Act, 1986*)

Agencies must appoint a Chief Information Officer (CIO) who must report directly to the agency head to carry out the responsibilities in the Paperwork Reduction Act, and the Clinger Cohen Act. (*OMB Circular A-130 "Management of Federal Information Resources," November 2000*)

Agencies shall establish clear accountability for information resources management (IRM) activities by creating agency CIOs with the visibility and management responsibilities necessary to advise the agency head on the design, development and implementation of information systems. (*Executive Order 13011 of July 16, 1996*)

Agencies shall delegate to the CIO the authority to administer all functions under this including:

- (1) Developing and maintaining an agency wide information security program.
- (2) Ensuring that the agency effectively implements and maintains information security policies, procedures and control techniques.
- (3) Overseeing personnel with significant responsibilities for information security. (*Government Information Security Reform Act, October 2000*)

Agencies shall designate a CIO who shall report to agency head to execute the responsibilities to:

- (1) Manage information resources.
- (2) Develop and maintain a strategic information resources management plan.
- (3) Develop and maintain (processes) to:
 - ensure that IRM operations and decisions are integrated with organizational planning, budget, financial management, human resources management, and program decisions.
 - develop a full and accurate accounting of information technology (IT) expenditures, related expenses, and results.
 - establish goals for improving IRM's contribution to program productivity, efficiency, and effectiveness, methods for measuring progress towards those goals, and clear roles and responsibilities for achieving those goals.
- (4) Maintain a current and complete inventory of the agency's information resources.
- (5) Conduct formal training programs to educate agency officials about IRM.
- (6) Ensure that the public has timely and equitable access to the agency's public information.
- (7) Implement and enforce records management policies and procedures.
- (8) Implement and enforce policies, procedures, standards and guidelines on privacy, confidentiality, security, disclosure and sharing of information.
- (9) Implement and enforce applicable government-wide and agency IT management policies, principles, standards and guidelines.
- (10) Promote the use of IT by the agency to improve productivity and efficiency.
- (11) Propose changes in legislation, regulations, and agency procedure to improve IT practice.

(Continued)

The Mandate for a CIO

(12) Assess and manage risks of major information systems initiatives through a process that is integrated with budget, financial and program management decisions, and used to select, control and evaluate the results. (*Paperwork Reduction Act, Sec.3506*)

Agency CIO shall be responsible for information assurance. Agencies shall appoint a Critical Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted at the discretion of the agency. (*Presidential Decision Directive 63, Section VII – Protecting Federal Government Critical Infrastructures*)

Terms

“Agency” means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency. (*44 U.S.C. 3502*)

“Information Management” includes “information resources management” and “process of managing information resources to accomplish agency missions and to improve agency performance to include the planning, budgeting, manipulating, and controlling of information throughout its life cycle.” (*44 U.S.C. 3502 and OMB Circular A-130*)

“Information Resources” means the information and related personnel, equipment, funds and information technology. (*40 U.S.C. 3502*)

“Information Resource Management” means the process of managing information resources to accomplish agency mission and improve agency performance. (*40 U.S.C. 3502*)

“Information System” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (*40 U.S.C. 3502*)

“Information Technology” means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (*40 U.S.C. 1401*)

CIO Responsibilities

Each executive agency head, in consultation with the Chief Information Officer and the Chief Financial Officer, shall establish policies and procedures to ensure that:

- (1) accounting, financial, and asset management systems and other information systems are designed, developed, maintained, and used effectively to provide financial or program performance data for financial statements of the executive agency.
- (2) financial and related program performance data are provided on a reliable, consistent, and timely basis to executive agency financial management systems.
- (3) financial statements support – (a.) assessments and revisions of mission-related processes and administrative processes of the executive agency; and (b.) performance measurement of the performance in the case of investments made by the agency in information systems.
(Clinger-Cohen Act, Sec. 5126 -Accountability)

Provides advice and assistance to the agency head and other senior management personnel to ensure that IT is acquired and managed consistent with agency priorities. (CCA, Sec. 5125)

Shall be involved at the highest level in the process and decisions [associated with the acquisition and management of Information Technology]. (EO 13011)

Shall have IRM duties as that official's primary duty; monitor the performance of IT programs, evaluate the performance of those programs on the basis of the applicable performance measurements, and advise the agency head regarding whether to continue, modify, or terminate a program or project; and annually, as part of the strategic planning and performance evaluation process:

- assess the requirements established for agency personnel regarding knowledge and skill in IRM and the adequacy of such requirements for facilitating the achievement of the performance goals established for IRM.
- assess the extent to which the positions and personnel at the executive level of the agency and the positions and personnel at management level of the agency below the executive level meet those requirements.
- in order to rectify any deficiency in meeting those requirements, develop strategies and specific plans for hiring, training, and professional development.
- report to the head of the agency on the progress made in improving IRM capability.
(CCA, Sec. 5125)

Develops, maintains, and facilitates the implementation of a sound and integrated IT architecture. (CCA, Sec. 5125)

Promotes the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency. (CCA, Sec. 5125)

Ensures agency compliance with and prompt, efficient, and effective implementation of the IRM policies and responsibilities, including the reduction of information collection burdens on the public.
(Paperwork Reduction Act, Sec. 3506)

Implements and enforces applicable policies on privacy, confidentiality, security, disclosure and sharing of information. (PRA, Sec. 3506)

(Continued)

CIO Responsibilities

Implements and enforces Government and agency IT management policies and assumes responsibility and accountability for IT investments. (*PRA, Sec. 3506*)

In consultation with the Chief Information Officer and the agency Chief Financial Officer (or comparable official), each agency program official shall define program information needs and develop strategies, systems, and capabilities to meet those needs. (*PRA, Sec. 3506*)

Develops and implements an agency wide information security program to provide information security for the agency's operations and assets. (*Government Information Security Reform Act*).

Reviews budget requests for all IT and national security systems, ensures that IT and national security systems are in compliance with Government standards. (*USC 10 Sec. 2223*)

Ensures that IT and national security systems are interoperable with other relevant IT and national security systems of the Government and the Department of Defense; and coordinate with the Joint Staff with respect to IT and national security systems. (*USC 10 Sec. 2223*)

Participates during all DON strategic management activities, including the development, implementation, and maintenance of agency strategic and operational plans and advises the Secretary on these matters. (*OMB Circular A-130*)

Monitors and evaluates the performance of information resource investments through a capital planning and investment control process, and advises the Secretary whether to continue, modify, or terminate a program or project. (*OMB Circular A-130*)

Implements and maintains a program to assure that security is provided for all agency information in general support systems and major applications. (*OMB Circular A-130*)

Thinking Strategically

The Clinger-Cohen Act mandate to establish a Departmental Chief Information Officer (CIO) provided the structure for the Department to address Information Management/Information Technology (IM/IT) needs at the enterprise level. The mandate to develop and submit to Congress an Information Management/Information Technology Strategic Plan focused the Department's attention on IM/IT issues and opportunities. On May 5, 1997, the Secretary of the Navy established the Office of the Department of the Navy Chief Information Officer (DON CIO) to provide top-level advocacy in the development and use of IM/IT and to create a unified IM/IT vision for the Department. As part of the initial standup, the Department created a CIO position and merged the Deputy Assistant Secretary of the Navy (Command, Control, Communications, Computers, Intelligence, Electronic Warfare, Space) (DASN C4I) functions with the CIO functions, creating a subordinate relationship of the CIO to the Assistant Secretary of the Navy (Research, Development and Acquisition). The DON CIO was charged with responsibility for the development of IM/IT strategies based on Office of the Secretary of Defense (OSD) guidance, policies, plans, architecture, standards, and for process reinvention support for the entire Department of the Navy (see Chapter 1, "The Congressional Mandate").

In the 1996–97 timeframe, CIOs both in and out of government had a short life expectancy. The DON was no exception. Three months after standup, the Department's first CIO, Dr. Marv Langston, who'd spent three years prior to establishing the DON CIO as the DASN C4I, notified the infant organization that he had accepted a new research position at DARPA. The Department began an executive search for another CIO. Four months later the second DON CIO, Dr. Ann Miller, was appointed. With the criticality of focused management attention on Y2K, shortly thereafter the decision was made to separate the CIO function from the DASN C4I function. In August 1998 the Secretary of the Navy named Dan Porter to the position of DON CIO. The leadership team now in place brought established networks, relationships and experienced change management strategies to help the young CIO office build its identity and value, and prosper and grow.

The new CIO team immediately set about identifying the scope of the CIO mission, structuring the organization to lead this effort, and connecting resources. An independent, external team was charged with conducting an assessment of the DON CIO mission, functions, and organization with regard to statutory, regulatory, and stakeholder requirements. They were also asked to identify opportunities to improve organizational efficiency and effectiveness. The team was comprised of two DON employees and two long-time DON support contractors, all of whom were experienced and proven leaders. Over a six-week period this assessment team reviewed statutory and regulatory requirements, reviewed internal DON CIO planning documents, interviewed CIO principals and external stakeholders, and synthesized information and developed recommendations. Simultaneously, an internal team interviewed DON CIO employees.

In the process of collecting information and identifying opportunities, it was very clear that DON stakeholders recognized the need for a Department level CIO. What was unclear was the mission, vision, and strategy for this organization. The current CIO organization was not perceived as playing an active role in significant Navy and Marine Corps IM/IT programs, the advisory boards and oversight structure did not appear to be functioning well, and CIO relationships with internal and external stakeholders were fuzzy. The current CIO organization was not structured to respond to the Fiscal Year 1999 DoD Authorization Act, ensuring that IT and National Security Systems complied with government and DoD standards, were interoperable with other government systems, were not duplicative within and between Military Departments and Defense Agencies, and were coordinated with the Joint Staff.

Other general observations collected from stakeholders in the assessment process provided rich fodder for helping to clarify the future path of the DON CIO:

- The CIO role in Information Assurance and Y2K was not well defined.
- There was insufficient Military representation for effective Fleet interface.
- There was a need for additional subject matter experts.
- There was a need to enhance corporate administrative and personnel policies and procedures.
- The CIO needed to take a leadership role for both information and knowledge.

A clear mission statement for the organization emerged from the array of information and process of developing relationships. With the CIO leading the charge, the DON would put information to work for our people—Sailors, Marines, and Civilians—in the operational forces, headquarters, and field organizations. But how would that be accomplished? What was the vision the organization would work toward?

THE VISION

The historical landscape of the IT world was built on presence: obtrusive technology with hardware and software controlled at the local level. IT decisions were made at the local level with a local context, thereby reinforcing the stovepiped, crisis-driven activity that tried to make sense out of the encroaching information chaos. Learned people searched for a standardized, stable environment.

INSIGHT

Each of us is separate and apart, bringing with us a unique set of assumptions and experiences. Yet essential to the success of any organization—or any country—is a shared vision and the commitment to achieving that shared vision. Historically, we've recognized the value of communicating; but today we realize the need for even more. Communicating must lead to shared understanding, so that leaders at every level of the organization can achieve a *connectedness of choices* as they respond to a rapidly changing, complex environment.

As the information age began to dawn in the mid 1990s, a quite different vision of the future began to emerge. People began to rely on virtual resources, trading stability for invisible technology and flexibility. The word ubiquitous came into its own, following on the heels of a recognized need for open standards and interoperability. The concept of continuous learning became a necessity in order to keep up with the incredible technology changes occurring daily. And “information needs” were beginning to change to “knowledge needs.”

Over weeks of collaboration, the vision and the areas of responsibility of the CIO began to emerge. Words and concepts drawn from experts, both internal and external to the DON started to build the DON IM/IT vision, beginning with the team, moving to the decision-maker, and addressing the culture of the organization:

- An integrated, results-oriented Navy and Marine Corps team characterized by strategic leadership, ubiquitous communication, and invisible technology.
- An effective, flexible, and sustainable DON Enterprise-wide information and technology environment that enables our people to make and implement efficient and agile decisions.
- A knowledge-centric culture where trust and respect facilitate information sharing and organizational learning.

During this assessment process, the CIO had undertaken an exhaustive examination of industry CIO agendas. The focus areas of those agendas were compared with government statutory and regulatory requirements, strategic DoD and DON documents with which they must be aligned, the activity currently underway in the DON in terms of focus and dollars, and the DON IM/IT mission and vision (see Figure 2-1).

As focus areas were identified for the DON CIO and related to efforts already underway in the DON system, there came the realization that all of these focus areas were interconnected, and that forward movement could only be achieved through a systems approach, and with an aligned vision focusing on all of these areas simultaneously. It was time to integrate this thinking into the strategic planning process.

The Department of the Navy IM/IT Strategic Plan mandated by Clinger-Cohen was due to Congress in the summer of 1999. While implementing a continuous cycle of strategic planning and performance assessment for IM/IT matters, a conscious decision was made to use the strategic planning process itself to gain the clarity of vision and strategy across stakeholders so important to the success of IM/IT in the Department.

THE STRATEGIC PLAN



The time-consuming process of developing the DON IM/IT Strategic Plan wove its way through the organizational and functional divisions of the Department, as well as up and down the chain of command. The document needed to be written at a level to make it real and viable, providing impetus for our organization to move forward, while providing the flexibility and tailoring essential for effective implementation at the organizational level, where implementation decisions are made.

The DON CIO worked with representatives from across the DON Enterprise and industry to create the first draft of this plan. By April 1999 the Strategic Planning Integrated Product Team had developed a draft plan that had been coordinated

with CIO team leaders and CIOs across the Department structure. In May, a Visionary Working Group comprised of executives from within the Military and Civilian structures of the Navy Department, Marine Corps, and Secretariat took a systems view of the Strategic Plan.

INSIGHT

The strategic planning process can be an important part of the change process. By involving people from every level of the organization throughout the process, and by identifying success stories—small victories that embodied the DON's vision for IM and IT—to publish in the Strategic Plan itself, the Department was operationalizing the Plan before it was published.

By July 1999 the plan had been vetted through the Secretariat, the Chief of Naval Operations, and the Commandant of the Marine Corps, and signed by the CIOs within those organizations. During the development of the plan, small victories—success stories—surfaced. The successes were initiatives underway that are achieving the DON's vision of the future. It was determined that applicable success stories would be included for each strategic goal. Through the use of teams and discovery of small victories, implementation was already well underway.

The Plan spelled out nine specific goals for FY 2000–2001. The first four goals addressed infrastructure, process change, capital planning, and the use of knowledge. The five additional goals interacted with the first four core goals. Since they were absolutely essential for mission success, they were addressed at the goal level. These are in the areas of technology injection, security, Y2K readiness, IM/IT competencies, and culture.

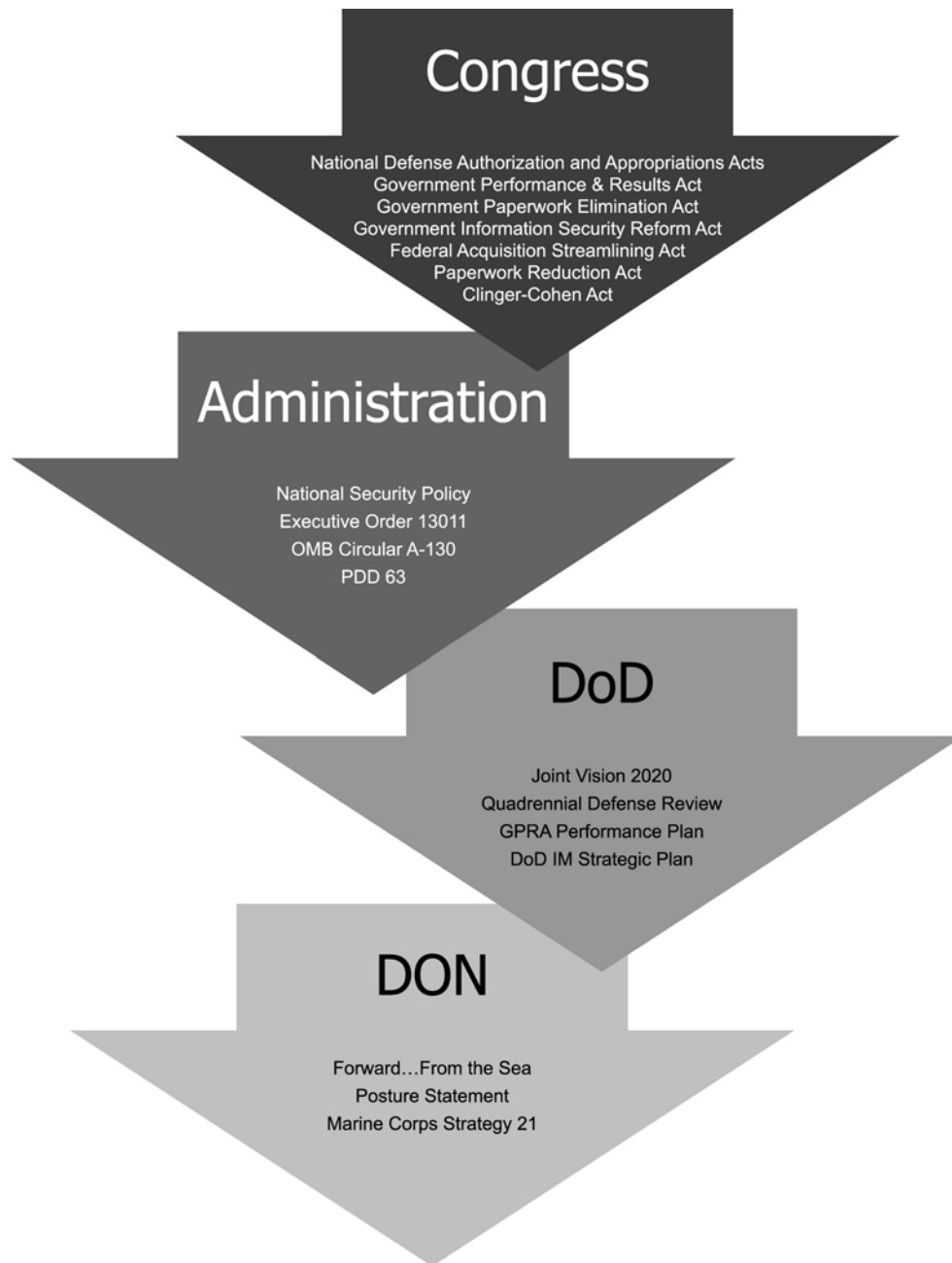


Figure 2-1—IM/IT Planning Process

These goals have been adopted by a number of industry organizations. The goals of the original Strategic Plan have been adjusted over the last three years to meet the evolving needs of the DON. The goal related to Y2K was successfully accomplished and removed from the current plan. The eight goals in the current plan are presented below.

Goal 1: Provide an information technology infrastructure that ensures knowledge superiority.

Develop, implement, operate, govern, and continually upgrade a global information infrastructure to provide transparent and seamless interoperability and end-to-end connectivity to all our people. Our entire warfare doctrine in support of Joint Vision (JV) 2010, JV 2020, Network-Centric Warfare, Expeditionary Maneuver Warfare, and Knowledge Superiority is based on access, interoperability, and security of our information and communications systems. The Navy Marine Corps Intranet (NMCI), seamlessly integrated with the Navy's shipboard IT for the 21st Century and the Marine Corps' Tactical Data Network, provides DON that capability. Based upon common architecture and technical standards for data, hardware, software, computing, and telecommunications, this infrastructure will result in the enterprise intranet, a component of the DoD Global Information Grid—a critical element of interoperability with joint forces and allied coalitions.

Goal 2: Infuse advanced information technology into warfighting and business processes.

Advance the improvement of warfighting and business processes by maximizing the contribution of knowledge and information technology. Process improvement coupled with innovation and technology infusion will increase mission readiness and enhance organizational effectiveness and efficiency.

Goal 3: Maximize the value and manage the risk associated with information technology investments.

Improve the management of IM/IT investments by directly linking them to improved combat capability and mission performance. The strategic requirement for quality information in a constrained resource environment increases the importance of making informed investment decisions. Better management of IM/IT investments will enhance combat readiness, maximize mission effectiveness, reduce total cost of ownership, and improve productivity.

Goal 4: Proactively encourage the creation and sharing of knowledge to enable effective, timely, and agile decision-making.

Implement knowledge management and eGovernment strategies to facilitate collaboration and information sharing that optimize strategic and tactical decisions, resulting in more effective and efficient mission performance. Knowledge management and eGovernment offer the potential to significantly leverage the value of IT investments and the intellectual capital of our people. Information technology and information management are essential, but alone are insufficient to achieve information superiority and, ultimately, knowledge superiority.

Goal 5: Exploit emerging information technologies to achieve information dominance.

Technology is a cornerstone for achieving knowledge superiority. The rapid transition and application of technology innovations improves mission performance. Partner with industry, other government agencies, academia, and our allies to identify and exploit breakthrough technologies.

Goal 6: Ensure information resources and critical infrastructures are secure and protected.

Ensure the reliability, availability, and integrity of information and information systems while guarding the privacy of our people. Implement critical infrastructure protection measures to protect, defend, and secure our mission-critical capabilities.

Goal 7: Build IM/IT competencies to shape the workforce of the future.

Provide Sailors, Marines, and Civilians with information management, information technology, and knowledge management skills and competencies essential for success in the information age. Facilitate the acquisition of skills that take maximum advantage of the richness of knowledge enabled by information technology. Provide training and education focused on both the IM/IT workforce and the IM/IT needs of the DON workforce.

Goal 8: Foster and incentivize a technology-enabled and information-rich culture.

Create a culture that will advance our workforce in the information age. Provide an intellectually stimulating and technologically attractive workplace for our Sailors, Marines, and Civilians. Incentivize innovative approaches and recognize IM/IT best practices that foster new patterns of work. Encourage open communications and implement an active outreach program that will ensure effective information flow and facilitate a knowledge sharing culture.

The DON IM/IT Strategic Plan has been distributed widely throughout all levels of the Department, formally through a direct mailing to all Echelon I, II, and III Commanders, and informally through teams and communities.

While the current DON IM/IT Strategic Plan has eight goals, the CIO organization has nine goals in its strategic plan. The first eight are identical to the DON IM/IT Strategic Plan; the ninth goal for the CIO organization is to lead implementation of the DON IM/IT Strategic Plan, addressing the infrastructure and resources needed to accomplish that goal. Toward achieving these goals, early areas of focus were identified. These areas are provided in Figure 2-2.

THE CIO ORGANIZATION

To accomplish initiatives in identified focus areas, the CIO set about creating a flat organization comprised of leaders who could, working through teams and communities, reach across the Department to pull together the best thinking in these areas. Three Deputy Chief Information Officers (DCIOs) would focus those efforts: one in the area of Infrastructure, Systems and Technology; one in the area of Y2K and Information Assurance;

and one in the area of Enterprise Integration. This strategy provided a Deputy who would focus full-time on the technology infrastructure to support creation of the Navy Marine Corps Intranet; a Deputy who would focus full-time on impending Y2K issues while looking at long-term security issues; and a full-time Deputy who could focus on long-term change through strategic planning, knowledge management, and IM/IT competencies.

In addition to the three deputies, a Special Assistant for Capital Resourcing would focus on capital planning, the CIO budget, and administrative support for the office. A senior IT counsel, sitting at the highest level of the organization, would ensure the organization's approaches, actions, guidance, and policy were consistent with the law.

Three and a half years into this program, the teams have shifted to meet the growing and waning requirements of the DON. For example, when the potential difficulties of Y2K were mitigated and the opportunities offered by eBusiness were recognized, the DCIO for Y2K and Information Assurance became the DCIO for eBusiness and Security, moving the important work of business process reengineering under this DCIO for focused attention. By the fall of 2001, the focus teams were in the following areas: Architecture and Integration, Capital Planning, Competency Management, Computing and Communications Infrastructure, Critical Infrastructure Protection, eBusiness/eGovernment, Enterprise Knowledge, Enterprise Licensing, Information Assurance, Librarian of the Navy, Organizational eLearning, Planning and Measurement, Policy Integration, Privacy, Section 508, Electromagnetic Spectrum Policy, System Registration and Certification, Technology Enablement Strategies, Technology Innovation, and Communications and Outreach.

As the DON began to focus on these areas, relationships among these initiatives began to emerge. The successful transition to the year 2000 was an essential and critical short-term goal. Given a successful crossing of that hurdle, other initiatives had long-term ramifications for the Department, and were very much dependent on the success of the Navy Marine Corps Intranet (NMCI) approach. At the core, NMCI proved to be the transformational initiative that would itself provide the baseline for knowledge flow, Web enablement, legacy migration, streamlined architectural design, enterprise governance, and a secure network environment, while shaping the workforce and reducing operational expenses. Figure 2-3 illustrates the transformational nature of NMCI.

While new requirements continue to emerge in response to the accelerating rate of change and increasing uncertainty and complexity of the environment, at the start of this book project, the teams were configured as follows:

DCIO for Infrastructure, Standards and Technology

- Architecture and Interoperability, including systems and operational architectures and data management.
- Computing and Communications Infrastructure, including standards, infrastructure architecture and the Navy Marine Corps Intranet.
- Systems Registration and Certification and Section 508, including statutory responsibilities for registering and certifying information systems and addressing accessibility issues.
- Electromagnetic Spectrum Policy and Management.

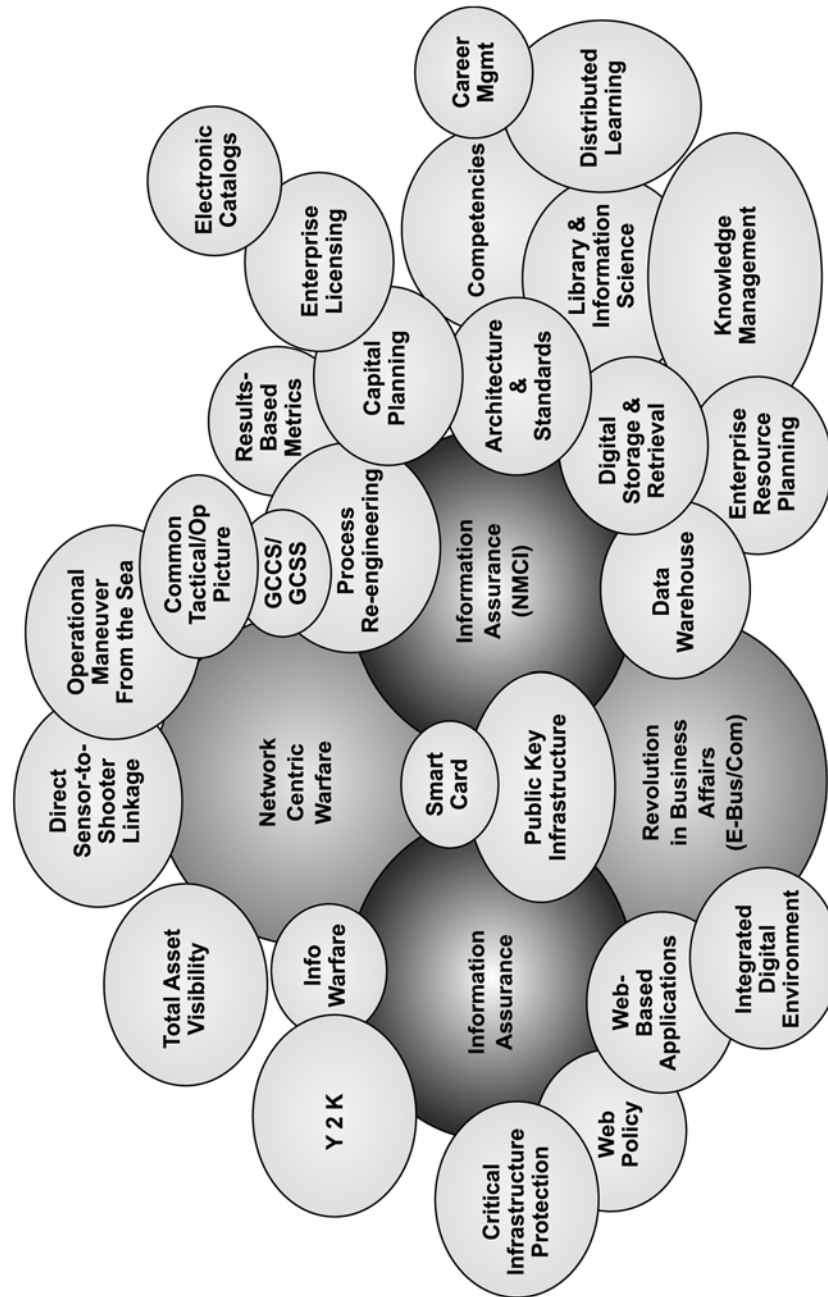


Figure 2-2
A Naval Information World View . . . It's all about information superiority!

- Technology Enablement Strategies including prototyping and pilot efforts, wireless issues, and technical consulting.
- Technology Innovation, including emerging information assurance and video technologies.

DCIO for eBusiness and Security

- eBusiness and eGovernment, including eBusiness strategies, business process reengineering, enterprise resource planning, smart cards, and balanced scorecards.
- Portals and Web Initiatives, including Web enablement, an enterprise portal, and electronic records management.
- Enterprise Licensing, including negotiating enterprise agreements for IT products.
- Information Assurance, including information security, public key infrastructure, network defense, biometrics, and Web and wireless security.
- Critical Infrastructure Protection, including assessing the vulnerabilities of the Department's critical physical and cyber infrastructures, reliance on local communities and the private sector for infrastructure support and developing indications and warning capabilities.
- Privacy, including ensuring personal privacy and assessing privacy provisions of IT systems.

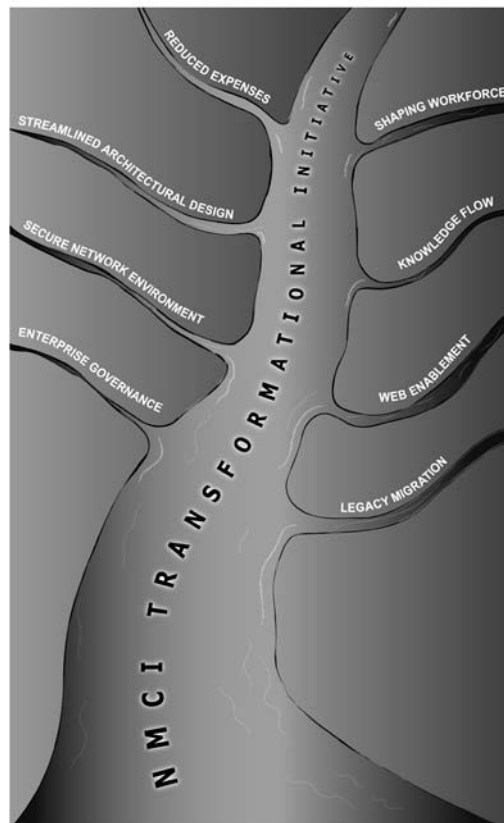


Figure 2-3—The river graphic illustrates the transformational nature of NMCI.

DCIO for Enterprise Integration

- Enterprise Knowledge, including Knowledge Management, content management, communities, and collaboration efforts.
- Competency Management, including IM/IT competencies, career path development, integrated competencies, and organizational eLearning initiatives.
- Liaison Officer, to include managing internal Departmental IM/IT leadership groups, relationships with auditing agencies, and external working groups and councils.
- Communications and Outreach, including the Department's IM/IT Web page, tool kits and corporate communications strategies.
- Planning and Measurement, including strategic planning, enterprise metrics, and IT investment practices.
- Department of the Navy Librarian, including library services.

While it was deemed important to create an evolving organizational structure that was flexible to emerging needs, there were also timeless and boundaryless factors identified that would be critical to the success of the DON IM/IT program, what we called Critical Success Factors.

DON CIO CRITICAL SUCCESS FACTORS

Critical Success Factors (CSFs) are major characteristics and factors that have contributed to making the DON IM/IT program a success over the past four years, and deal as much with the way specific initiatives are implemented as the initiatives themselves. Taken together, they significantly impact the ability of the DON to successfully execute the IM/IT Strategic Plan.

These Critical Success Factors have facilitated the success of DON CIO initiatives. The icons listed beside each factor below appear throughout this book where specific factors have been important to the successful implementation of specific initiatives. Specific locations may be found in the index.



Leadership: DON CIO leadership adopted an internal collegial working environment and developed an external strategy that supported Department-wide leaders and workers in their implementation efforts. Leadership also set examples of openness, cooperation, and close collaboration with outside individuals and organizations.



Managing Change: Every organization must adapt to its changing environment. New technology, new missions and new global political and Military situations demand that the DON's culture, capabilities, and processes be continuously reviewed and recreated as needed. Thus the ability to identify and overcome barriers to change, coupled with an effective change management program, becomes critical to the DON mission.



Timing: Influencing a large organization requires that the sequence of actions and the speed of change be carefully planned and implemented, within the constraints of the culture and external events. The DON CIO carefully thought through its strategy, focus areas, sequence, timing, and execution of major actions to maximize the probability of success.



Quality: A significant part of the DON CIO's change strategy deals with recognizing quality throughout the organization, rewarding that quality, and diffusing it throughout the DON. In addition, DON CIO adheres to a very high standard of quality for all IM/IT products and services.



Systems Approach: The DON CIO adopted a broad systems view of the Department and its responsibilities across the Department. This perspective allows DON CIO to focus on the most important issues and to understand differing views on many issues and problems. It also recognizes the payoff of a long-term view of desired results, and encourages a balanced understanding of the overall needs of the DON.



Service: In addition to setting policy and strategic direction, the DON CIO recognizes that it exists to provide a service to the line and staff organizations throughout the Department, helping them to achieve current and long-term mission success, i.e., defense of the nation.



Technology: Clearly technology is a prime thrust of the DON CIO. Always viewed as an important resource in accomplishing mission objectives, technology is not considered an end in itself. Policies were developed that ensured technology was used most efficiently, effectively, and securely in support of organizational objectives. Ideally, the best technology is invisible and ubiquitous, while leveraging human competency and supporting decision-making throughout the Department.



People: A recognition of and strong reliance on the importance and quality of the Department workforce has consistently helped facilitate communication and create a widespread understanding of what the DON CIO was trying to accomplish. Much of the needed change had to occur through a change in culture—the way the work gets done. This can only occur through and by people—their attitudes, perceptions, and willingness to try out new ways of getting the work done. See Chapter 9, “Managing Change,” for additional discussion. In response to the changing environment, people must learn new techniques, use new tools, and develop new principles and behavior patterns.



Creativity and Innovation: Meeting new challenges in a dynamic, uncertain, and complex environment requires the continuous insertion and implementation of new ideas. These ideas emerge from within and without the DON CIO framework, with the DON CIO playing a major catalyst role in the stimulation and integration of these ideas.



Sharing: The widespread sharing of ideas, opinions, information, and issues plays a large role in creating coherence in the Department's response to new policies. Embracing expertise throughout the organization, the DON CIO worked with other organizations to develop guidance and policy, generating CDs and other informative resources, and distributing them to personnel throughout the Department, other Federal agencies, and to our industry partners. This practice allowed all concerned to understand the need for change and how they could participate. Affirmation and validation occurred both internally and externally.



Freedom and Flexibility: Providing resources and facilitating the skills to support new ways of doing business help empower decision-makers at every level of the chain of command. Effective strategy implementation requires many rapid, complex decisions that can only be made locally in the field. In addition, DON CIO professionals had the freedom to make decisions and take the actions needed to do their jobs within the context of local needs. Such freedom and rapid actions greatly enhance the DON CIO's ability to effect change and provide true support to the operating units.



Communication and Persuasion: These were fundamental to achieving DON CIO goals. Department organizations needed to understand the reasons and benefits of the DON IM/IT policies to accept and implement them. This required close and effective communication with a great many individuals and organizations throughout the DON Enterprise. Personal meetings, conferences, presentations, workshops, telephone and video-conferencing were all used frequently to facilitate understanding and bring people into the world of the future. See Chapter 3, "Connecting Across the Enterprise," for additional detail.



Team Approach: Because of the complexity of the challenge facing the DON CIO and the speed of change occurring throughout the Department, it was essential to take a team approach to achieve all objectives. Teams, Communities of Practice, task forces, and other vehicles of collaboration were established that encouraged hundreds of personnel to work together, solve problems and share experiences.



Continuous Learning: Continuous learning became a daily routine within the DON CIO, and the DON CIO became a Department champion for eLearning. Over the past four years Y2K, knowledge management, and computer security all came to the forefront and presented new problems and opportunities. These and many other challenges required new ideas, solutions and approaches. Basic assumptions were questioned, experts sought out and listened to, and policies and implementation strategies developed on a seemingly short-term basis. As environmental change accelerated, the need for new workforce skills and capabilities increased, and eLearning offered solutions.



CSFs

Hard Work: As always, hard work and dedication, backed by integrity and a strong value set, served as the foundation for external credibility and trust: the two essential characteristics for influencing others and managing change.

Many of the above factors are mutually supportive. For example, freedom, flexibility, continuous learning, working in teams and sharing, taken together form an interconnected system that generates trust, motivation and hard work, which cannot help but lead to success. Supportive leadership, high quality standards, a systems perspective and an attitude of service to others create an image to the outside world of a positive, dedicated, rational, and competent organization. This image goes a long way toward cooperation and collaboration with customers.

COLLABORATING WITH OUT-OF-THE-BOX THINKERS

In October 1999 the Under Secretary of the Navy hosted an Expert Forum to address consequence management (both in the light of Y2K and future events) and explore ways to consider unknown unknowns. This forum provided the opportunity to validate and extend much of the strategic thinking driving the DON CIO. Held at the Naval War College in Newport, RI, the Expert Forum brought together senior DON leadership and world-class thinkers with diverse areas of expertise. These thinkers included Edward DeBono (the father of lateral thinking), Catherine Allen (CEO of the Banking Industry Technology Secretariat), Bernard Boar (author of *The Art of Strategic Planning for IT*), Michael Bayer (Chair of the Army Science Board), John Petersen (President of The Arlington Institute) and Margaret Wheatley (author of *Leadership and the New Science*). This eclectic group searched for new ideas, insights, perspectives and actions to better prepare the DON to address Y2K unknown consequences in particular and unknown unknowns generally.

Consensus on ideas did not occur, nor was it asked for in this one-day event. What these thoughts did do is seed additional thinking and surface new ideas regarding the future direction of the DON CIO. There is a consistent relationship between many of the thoughts from this session and the DON initiatives shared throughout this book. In the further spirit of sharing, a number of these ideas are recorded below. Although the terms “need” and “must” are used extensively in this material, **these ideas and thoughts are those of individuals, and do not, nor are they intended to, represent the position of the Department of the Navy.**

Present and Potential Future Environments

The first thoughts that emerged from this brainstorming session dealt with what the present and future economic and business environments look like. These thoughts are presented in the following paragraphs. Ideas address a broad spectrum of areas, ranging from economics and politics to culture, and from technology to education. This section includes out-of-the-box thinking that is diverse and as eclectic as the people participating in this exercise.

Thoughts on Economic and Political Trends. The global economy is based on interdependence. The increasing economic disparity among nation states and sub states is developing two world classes: the haves (those adapting technology and globalization) and the have-nots. IT competence is an indicator of this division. This disparity will have an impact on rational decision-making during times of uncertainty and crisis.

National boundaries are becoming more porous because of economic, cultural and social changes, and there is evidence of systems (business, people, information, finance) operating across, and in many ways independently of, national structures. We need to look beyond nations to global systems that transcend nations, forming new international strategic alliances. Shifting sources of power offer the opportunity for change in third world countries, but also the danger of small disturbances exploding into major catastrophes. New political relationships are forcing rethinking of how we exert influence. On the domestic front, there is a need to understand where the domestic political agenda will take us, and for strong leaders with ideas that inspire and unite.

Thoughts on Information Technology. As dependence on IT increases, it is becoming increasingly viewed as a service. The emphasis is on better value concepts supported by IT, not created by IT. This new way of thinking is contrasted by many organizations moving to stovepipe IT into technology-centric components, de-linking it from operations. This IT elitism may create intellectual and corporate blind spots to potential emerging usage and technologies. Issues that need to be addressed include what is best for IT interactions, what is best for human interactions, and how do we best connect IT and human interactions. The increase of virus attacks is of great concern.

Thoughts on the Nature of Warfare. Information technology is changing the fundamental nature of war. Interconnectivity provides the vehicle for electronic warfare as well as massive psychological warfare. Warfare will be held on a total information basis, much like a chess game, with not enough time to actually deploy forces prior to elimination, and the moves based on no common ethical base. We must converge our cyber and physical warfare doctrines. The question to ask is: When does cyber warfare lead to the use of physical force (not either or)?

Thoughts on Internet and Communications. The Internet is rapidly becoming a utility, with infrastructure changes underway to expand cellular and satellite usage. The next-generation Internet offers the opportunity for instant processing, improved global access and ubiquitous communications. The new Internet culture is driving value shifts, and influencing how people see events. The force of public opinion is more powerful than ever before. Rumors and opinions are quickly spread around the world, setting up the public as a Greek chorus and translating into action in the market place. For example, the Internet is enabling politicians to reach voters one-on-one, opposing forces within authoritarian governments to make information widely available, and enabling mass customization.

Use of the Internet is developing multitasking capabilities in our connected youngsters. But with it comes the loss of personalization and the isolation of people. [This concept of isolation is part of a pattern that surfaced throughout this event.]

Thoughts on Knowledge. There is an economics of knowledge coming which is causing a major shift in the way we do business. There is a new recognition of the value of knowledge and wisdom over information and data, and questions of how to convert information to knowledge. This value is found in intellectual capital (the venture capital of ideas) and social capital (the stuff that connects us, builds on relationships and provides the ability to make sense of knowledge when we receive it).

Information flow and knowledge sharing are becoming more and more important, with value placed on what you share, not what you collect. One methodology is storytelling. People learn from storytelling and it provides a sense of the whole and provides context in complex organizations. Leaders need to encourage sharing at all stages of the process and to design knowledge systems to collect and sift through data and information, organizing and arraying this information for ease of consumption. Effective sharing builds on trust. It is necessary to create an environment where intranet products support group discussion and collaboration is honored.

The economics of knowledge and need for sharing is driving new organizational structures. Virtual and human intermediation is developing a new profession focused on the business of connecting those that know with those that need to know. New cross-links and discussion methods are supporting development of Communities of Practice and of Interest. There is a need to develop methods to capture tacit knowledge and facilitate enterprise-wide knowledge intelligence systems. Issues that need to be addressed include how to maintain an expert's value as information is shared, the veracity of knowledge given the short time frame for decision-making, and the need for time to share knowledge. We must connect IT, IM and KM as critical elements of the warfighter mission.

Thoughts on Social Change. Interconnectivity—and the resulting complexity—is affecting individual identity, promoting the lack of human contact and causing the breakdown of normal relationships. Chaos, uncertainty and change are threatening historical loyalties to social and religious systems. All this is causing overreaction to subtle perturbations and creating a thirst for simplification of life. People are self-organizing around regions and localities, both functionally and virtually, to create extended families. People have a desire for more control in their lives, providing openings for paternalism and patriarchal (or matriarchal) social formations, the emergence of new religious leaders, and increasing the potential for dictatorships. Spiritual elements are moving into the workforce, causing a confusion of roles and development of new value sets. This is accompanied by an emphasis on spirituality issues, such as increasing fundamentalism. Emerging new moral standards are responding to the importance of emotion and the need for instant gratification.

Thoughts on Culture and People. There are two opposing forces affecting cultural change: escalation of the need for cultural heritage, and the blurring of cultural heritage. Increased localization of special interest groups and development of Communities of Interest that cross cultures are two rising trends. The ability to use information is creating a new information literate class of people with a higher standard of living. In the U.S., the age of marriage is rising and birth rates are decreasing. Cloning concepts receive passionate discussion. The aging U.S. population is placing strains on the retirement system, with potential insufficient funds to pay pensions.

The continuing decline in unemployment levels will result in a real-time shortage of personnel, particularly for the Military. The type of work is changing, with the need for more designers and fewer analysts, and the need to develop a new concept of employment, particularly for entry-level jobs. Fads, trends and hysteria produced by the Internet are affecting individual thinking. There is an increased need for psychological leisure, not just travel leisure. The messages of music are increasing in importance.

Thoughts on Education. Education is increasingly seen as out of touch with society. Public secondary schools are displaced by a coalition of concerned parents and corporations that are concerned with poor performance. There is a growing educational gap between classes, and a need to accelerate development of new concepts and systems, with technology leading the way. There is an inability of the education system to help people understand how to provide value. Young people wish for a prolonged youth culture—many going abroad to study—and as they finally enter the workforce are searching for more meaning. Ninety-four percent of youngsters rank achievement as their greatest need.

Consequence Management

A second thrust area of the Expert Forum dealt with consequence management. The thoughts shared in this section are rich in potential opportunities for any organization (government or non-government) operating in the new global knowledge economy. The world—an increasingly complex system—is in a continuous state of change. The rate of change of complexity is rapidly moving beyond our ability to understand or deal with unintended consequences. Traditional analytical techniques don't help with non-linear complex systems. All these changes demand new ways of looking at the skills, processes and organization needed to handle the unknown unknowns of tomorrow's world.

Thoughts about New Skill Sets. Critical Thinking Skills—new, unusual, tried and tested, bizarre—are becoming skills of major value. Critical thinking, systems thinking, creativity and innovation, possibility thinking, well-honed intuition and new ways of knowing will position members of the workforce individually and collectively as walking, breathing consequence managers. Critical thinking helps bound messes and promotes integration of capabilities. *Systems thinking* provides the tools to identify nodes, connectors and influence points in systems, leading to the design of ways to influence these. *Creativity and innovation* are essential to continued growth, including learning how to discard old ideas with as little penalty as possible. Creative hypothesizing is key to *possibility thinking*. You can only see what you are prepared to see. Data and information must be viewed through possibility. We should actively utilize new intuition-accessing methods that are intrinsically non-linear to get at both the essence and implications of complex systems, and learn to respond to discomfort. Decisions must be made in instants and intuition will be as important as analysis.

Sensing must become a core competency and recognized as a positive asset for career development. Sensing provides richness over the analyzing of single point convergence. Early sensing of changes is an important skill that improves our agile response to highly variable situations.

Scanning is a second competency. With this skill, individuals can scan the horizon for early indicators of specific areas of concern and potential problems, facilitating connection of cross-network, cross-functional, cross-organizational patterns. Scanning capabilities are key to development of a process for identifying trends and behavioral changes, and direct networks can be set up between scanning teams and response units during times of crisis.

Patterning builds on sensing. This skill is used to identify underlying trends and combinations thereof and look for anomalies. Patterns need to be imagined before they can be seen, so the use of lateral thinking drives pattern-sensing techniques. Advanced IT is an enabler for pattern recognition.

Finally, there is **Storytelling**. Whenever someone sits in a complex organization they will see a situation differently. Telling stories provides context and a sense of the whole. Effective stories built on the cultural value set have a long organizational life span.

Thoughts about New Ways of Perceiving. Ways of perceiving included thoughts about engaging different viewpoints, perception management, and unintended consequences. Those who are involved in the process inevitably become co-opted by the process—we must continue to engage those outside of the process to explore different ways of thinking about problems. This includes drawing on a variety of perspectives: economic, cultural, political, international, religious, etc. We must explore non-traditional ways of thinking and seek the perspective of the Internet generation, who perceive events through a different value system.

The perception of society is largely influenced by the news and entertainment media and is independent from reality issues. We need to pay as much attention to perception management as to technological issues. Think of the various groups such as Congress, the media, the public, foreign governments, etc. and what their concerns will be and how to handle those concerns. Public Affairs must become a core competency of the Defense Department. We need to send stronger signals to the outside community, building public confidence in our ability to handle emergencies and do contingency planning. As we begin to understand the effect of perception, we need to simultaneously explore the **unintended consequences** of both our actions and the perception of our actions. For instance, collateral dangers from minimizing problems include blocking identification of solutions and new trends.

Thoughts about Organizational Efficiency and Effectiveness. The result of consequence management must remain **mission accomplishment**. We must constantly ask what are our long-term and strategic goals and how does our short-term response affect those goals (positive or negative). The traditional mode of thinking creates products ... we then get wedded to those products. We need to focus on **agility** and focus response teams on those things we are not prepared to handle, trying to define the potential directions and mass results, and remain receptive to mid-course correction. People in a rigid culture need to be trained for agility, leveraging the approach used in times of war. One prepares for emergent situations generically. The job of an organization is to use today's event to prepare for the next event ... we solve today's problem as a collateral issue while trying to capture the lessons and essence for tomorrow. Agility carries with it the idea of redundancy ... having some slack to be robust and agile. **Relative inefficiency** is a necessary component of

effective complex systems. **Adaptability** is also important. *Position thyself for unknowns and react as they emerge; those who can adapt are victorious in wars or other situations* (Sun Tzu). All actions cannot be preplanned; therefore, consequence management is all about adaptability and agility. The focus is on better ways to react, rather than trying to prevent.

As all these changes occur, we move toward an open society, with increased transparency individually, nationally and across coalitions/alliances, and the accompanying loss of individual and corporate privacy. **Organizations need to restructure** to prepare for/embed change behavior and ensure valuing new knowledge elements of warfare and defense, and operationalizing communications in every warfare area. As we move from centralization to decentralization, we need to change our control mechanisms to coordination mechanisms, yet think in an enterprise fashion. Finally, regarding **measurement**, the temptation to measure consequence management immediately is great. We historically look for a clear explanation of the near-term and long-term results of our actions. Consequence management results are rarely measurable or clearly good or bad. The world isn't that clear cut and inherently cannot be predicted; only the future will tell. We need to develop new ways to track success.

Thoughts about Knowledge Systems. **Sharing and Collaboration** are essential. The biggest capital asset in consequence management is trust and how much it is spread around. Processes for thinking together, if they're truly collaborative and not just listening to experts, are the source of trust. We need to create cross-links and discussion methods to share thinking and ideas with others who may also be impacted by unknowns. We must build **Communities of Practice** and **Communities of Interest** covering the full spectrum of warfighting and warfighting support to assure availability of our intellectual capital when/as needed. We need to create intranet products that facilitate group discussions and exploration, plus have the capability to search broadly for insights and conclusions from prior chats and studies. We need to create **virtual capability** based on subject matter for anyone to reach out and grasp, without boundaries or borders, and without pride of authorship. We need to build a toolkit available across the Enterprise that integrates lessons learned and successes and points of contact tied to intellectual systems which can slice, dice and build patterns and relationships between data and information.

Thoughts about Learning and Educating. "We train for the known, we educate for the unknown." While training is necessary, education is essential. We need to redesign our education system to teach "how to be wise" and how to provide value. We need to significantly reevaluate the relationship between technology and education and assure educational material is current and relevant. We need to empower Sailors, Marines and DON Civilians in the new world with the tools to survive in technology-driven warfare, both physically (hardware and software capabilities) and mentally (thinking skills). We need better visualization tools that allow improved understanding of the thought process.

Thoughts about Cultural Change. We need to develop a culture that is inclusive, highly diverse and open, where we invite contributions from everyone and build trust from working together on important projects. This culture must be based on shared meaning. Navy/Marine Corps myths must be challenged ... the most dangerous thing is to believe our own myths.

CONCLUDING THOUGHTS

Thinking strategically allows for both the solving of immediate problems and the transference of knowledge gained to address emerging or even yet unforeseen problems. For example, successfully addressing the Y2K problem, the broader issues of protecting our people and our critical infrastructures became apparent. Strategically thinking through Y2K issues sparked development of an innovative Critical Infrastructure Protection effort that broadened the Department's security horizons to additionally focus on critical dependencies and single points of failure within the local communities and private sector firms that our Military bases rely upon to conduct their operations.

New ideas continued to emerge every day, as teams, communities and forums focused on this important work of the Department. The vision was clear, the strategic plan in place, the organization structured, and the critical success factors embedded throughout. The DON CIO set about building the networks and relationships that would enable success.

Connecting Across the Enterprise

Developing a close partnership with Information Management/Information Technology (IM/IT) leaders in both the Navy and Marine Corps has been instrumental in creating an Enterprise focus which crosses organizational boundaries. This was visibly evident in development of the Department-wide IM/IT Strategic Plan which integrates goals and objectives and harnesses leadership commitment from each of the services. An Enterprise infrastructure built on the foundation of the Navy Marine Corps Intranet (NMCI) is also a product of this collaborative relationship. The Department of Navy (DON) IM/IT vision of an integrated, results-oriented Navy and Marine Corps team is steadily becoming a reality.

The CIO organization—situated at the highest level of the DON Enterprise and in the sphere of policy, strategy, and oversight—operates at the behest of the Department. While in a leadership role, the DON CIO approach is as a service organization. Its mission of *putting information to work for our people* can only be accomplished with a full understanding of the current and future needs and requirements of people at all levels of the Department. In short, an organization charged with guidance and policy cannot operate in a vacuum, and must maintain a continuous dialogue with its stakeholders and customers. The success of the DON CIO in *putting information to work for our people* is accomplished through connecting people.

TEAMS AND COMMUNITIES



Integrated Product or Process Teams (IPTs) were used to develop and facilitate implementation of broad-based IM/IT initiatives. IPTs are described as groups of individuals who have complementary skills, who are committed to a common purpose and performance objective, and who hold themselves mutually accountable. While there are many descriptions and interpretations of IPT and team, in practice the terms are often used interchangeably. What is important is what the team does, and how the team does it. IPTs are information and knowledge teams. They provide the professional work needed to perform special studies, solve complex problems or acquire products such as combat weapon systems. IPTs bring together the right people, with the right backgrounds and competencies, to accomplish a task.

For example, an IPT was chartered by the DON CIO to examine the issues and identify policies and practices to support the DON workforce. Membership spanned the Marine Corps, Navy claimants, and Secretary of the Navy organizations that were stakeholders either by virtue of their sizeable IM/IT/KM workforce, or their responsibilities for human resource policy and procedures. The IPT sought input from sources across the public and private sectors, and identified Enterprise-wide workforce requirements for the FY2000–2005 timeframe. Their actions included developing the *DON IM/IT Workforce Strategic Plan*, refining DON CIO guidance on inherently governmental and non-inherently governmental functions, and creating the *DON Civilian Career Path Guide for the*

Management of Technology, Information and Knowledge. For more information on this IPT see Section 6.1 “IM/IT Workforce Competency Management.”

As a second example, the Data Management and Interoperability (DMI) IPT, consisting of data management experts from over 40 Navy and Marine Corps commands, completed a year-long effort focused on defining the policy, processes, and tool requirements to support development of a data architecture. The DMI IPT addressed three major areas: (1) data management policy, (2) architecture and standards, and (3) repositories and tools. Each of these three areas is key to establishing an Enterprise data management program.

Another form of “team” or sharing groups is communities. Using the power of information technology to create an environment that is conducive to sharing knowledge, the DON CIO championed development of communities of practice and communities of interest to assist in leading implementation of the IM/IT Strategic Plan. Communities of practice are formal or informal structures that facilitate knowledge sharing among individuals with common interests. Connected by the Internet, these communities meet virtually—and occasionally face-to-face—to solve problems, share lessons learned, and promulgate best practices. In this environment, individuals around the globe have access to one another to share the knowledge that comes from experience. As a result, communication among communities can be parallel, continuous, and seamless, rather than sequential, scheduled, and segmented. A new set of expectations and practices is emerging; people expect to be able to interact and obtain the knowledge they need, when they need it, no matter where they are. Communities that interact virtually are helping to make anytime/anywhere access to knowledge possible.

The Knowledge Management Community of Practice (KM CoP), the first formal community in the Department, evolved from two KM conferences sponsored by the Navy Department in late 1998 and early 1999. Facilitated by the Navy's Post Graduate School in Monterey, CA, these conferences brought together early KM champions and innovative thinkers who recognized the opportunity KM offered. From these beginnings, the KM CoP has grown to include over 300 members representing 60 different DON organizations. The KM CoP is focused around knowledge and built on developing relationships among participants. It is supported by a virtual technology system that brings the latest findings of the American Productivity and Quality Center (APQC) and Institute for Knowledge Management (a group of 40 industry and government organizations focused on KM research and run by IBM) into the hands of CoP members.

As a third example, the Investment Practices Community of Interest (COI) consists of a group of individuals who have come together informally outside of organizational structures to share knowledge about the development, implementation, improvement, and success of IT Portfolio Management and Investment Practices in their organizations. Current membership, at over 250, includes participants from the DON, DoD, Civilian agencies, and industry.

EVENT INTERMEDIATION



Communities of Practice and Communities of Interest serve an intermediation, or knowledge broker, role. Another type of intermediation deals with events. In a complex non-linear system, where change occurs in an uneven fashion, a “plateau shift” can be precipitated through formal large enterprise events. For example, when the DON was faced with the rapidly approaching deadline of the year 2000 (Y2K), it conducted a Y2K Virtual Town Hall. The Town Hall, hosted by the Under Secretary of the Navy, brought together 35 senior leaders from across the Navy and Marine Corps, representing every major organizational element facing Y2K mitigation. The event was broadcast live over the Defense network, local based cable systems, via video teleconferencing and Internet streaming, and videotaped for worldwide dissemination. Questions were received during the event via telephone and e-mail. Every leader was in the spotlight for immediate answers, and all these answers and the following exchanges were shared live across all organizational and functional levels.

In short, after several months of anticipation and planning, Enterprise attention was focused on Y2K at one place and one point in time. From that event, the Department achieved a plateau jump in both defining where it was in Y2K remediation and actually accomplishing this remediation. Additional value was accrued in the perceived—and legitimate—identification of the Department as a leader in mitigating potential Y2K problems.

Major DON intermediation events for Knowledge Management and eBusiness were held in August 2000 and 2001. These Knowledge Fairs, built on a model used by The World Bank, carried the commitment from senior leaders, provided the opportunity for personal sharing of successful KM and eBusiness initiatives, and included short demonstrations and learning experiences. The learning was escalated through the capture on video and CD of the messages, initiatives, and points of contact for those initiatives, adding context to explicit documentation through personal conversations and short recorded visuals.

The DON's Connecting Technology (CT) symposia, held twice a year (once on each coast) foster the exchange and sharing of information essential for interoperability at all levels. CT connects the DON IT workforce with current technology, contracting, and technical information, as well as with DoD leaders and industry experts who drive technology acquisition and implementation. CT truly meets its goal of “Connecting People” with over 1,200 IT professionals attending from all over the world. A broad array of topics is selected to keep pace with the rapid speed of technology and policy, along with speakers who are recognized leaders in their fields. CT includes over 100 exhibits from DON commands and companies doing business with the DON. The latest in technology and service offerings are exhibited, and DON personnel have the opportunity to explore potential solutions.

FORUMS



The Y2K Virtual Town Hall was only one DON Y2K event. In addressing the extremely complex and Enterprise-wide challenges facing the Department as the year 2000 approached, the Department of the Navy Chief Information

Officer made extensive use of various forums to stimulate intellectual dialogue, explore potential management strategies, and develop innovative approaches to solve complex organizational problems.

Early in the Y2K process, the Department realized that the successful transition to the year 2000 was dependent upon the proactive involvement of the Department's senior leadership team. There was a clear recognition that Y2K was a "CEO" issue, not just a "CIO" issue. The Department held an Industry Forum to allow the Under Secretary of the Navy, the Vice Chief of Naval Operations and the Assistant Commandant of the Marine Corps (the "COOs" of the Department), the Chief Information Officer, and other senior Navy and Marine Corps leaders to meet and discuss management strategies and innovative approaches with industry counterparts. By bringing together a diverse group of senior leaders from industry, to include, Gartner Group, Fannie Mae, Compuware, Computer Associates, Virginia Power, Lockheed Martin, the Arlington Institute, and Kapos Associates, the Department's leadership team was able to engage in the far reaching and extremely productive exchange of ideas over the course of a single day. This encounter generated significant management strategies and a shared understanding that benefited both government and industry attendees.

As the year 2000 approached, and system remediation efforts were being wrapped up, the Department of the Navy turned its attention to consequence management. Recognizing the value of its Industry Forum in generating new ideas and knowledge, an Expert Forum was held at the Naval War College in Newport, RI, to explore ways to prepare for and effectively transition into the new millennium. The fact that Y2K problems could conceivably occur in an unknowable number of locations, with potential impacts and interrelationships not even considered, required that thorough examination be given to addressing and resolving "unknown unknowns." Senior Department of the Navy leaders met with world-renowned thought leaders for an intensive day and a half session. The results of this session are included in Chapter 2, "Thinking Strategically."

AWARDS



During the Knowledge Fairs and Connecting Technology symposia, DON eGovernment awards are presented to recognize project teams whose successful initiatives are leading the exchange and sharing of information across organizations. Presented by the Secretary of the Navy and Flag Officers from the Navy and Marine Corps, these awards, consisting of a plaque and a citation read during the formal awards ceremony, are held in high esteem by the DON IM/IT workforce.

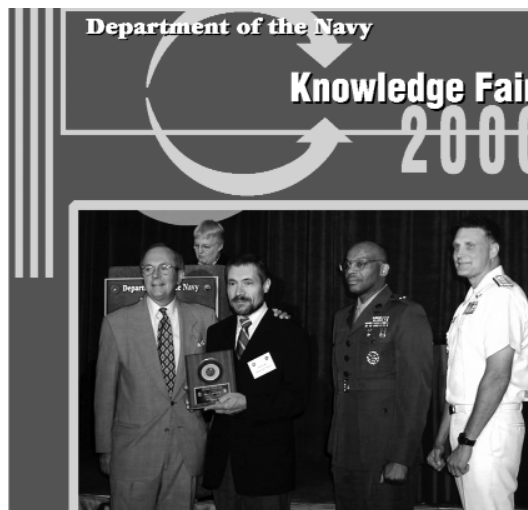
For example, one such award was presented to the Global War Game KM/IT Team. This team contributed extensively to operationalizing the Knowledge Management concepts in Joint Vision 2020 and Network Centric Operations. Network Centric Operations recognize that Military conflicts will increasingly depend on, and revolve around, information and communication matters. Information-age modes of conflict will be largely about "knowledge"—who knows what, when, and where. The Global War Game KM/IT team focused during the 2001 wargames on how to operationalize Network Centric Operations



Figure 3-1—The Secretary of the Navy, Gordon R. England, is greeted by roving robot while touring the Knowledge Fair.

and its underlying means to exploit and distribute information to dramatically improve our ability to be well informed and to share and exploit our knowledge.

As a second example, the DON eBusiness Operations Office won an award for leading implementation of eBusiness in the Department of the Navy. This office, headquartered at the Naval Supply Systems Command, was established in May 2000 to serve as a clearinghouse for fresh eBusiness ideas for Navy and Marine Corps business processes. In April 2001, from more than 360 submissions, it selected eight Navy and Marine Corps eBusiness pilot projects to be funded during the fiscal year. The selected projects critically evaluated the latest technologies in the public and private sectors and demonstrated their viability and usefulness across the full range of Navy and Marine Corps functional areas. One of the pilots, the Medical Appointing Pilot Project, has been adopted for DoD-wide use.



*Figure 3-2—
Former Under Secretary of the Navy
Jerry M. Hultin presents
DON eGovernment awards.*

Every award winning team deserves recognition here, so all DON eGovernment awards and recipients are listed in the following tables.



DON eGovernment Awards

Award Category

Award Recipient

Presented at the DON Knowledge Fair, August 2000

- | | |
|---|--|
| Most Scalable KM Solution | • Network Centric Innovation Center
Commander 3rd Fleet, Stennis
Battle Group Carrier Group 7
Space and Naval Warfare
Systems Command (SPAWAR) |
| Outstanding Cross-Organizational
Knowledge Sharing | • US Joint Forces Command |
| Leading Knowledge Portal Concept | • Knowledge Home Port |
| Innovative Knowledge Sharing
in the Marine Corps | • Marine Corps Systems Command
TIGER Project |
| Outstanding Collaborative
Knowledge Sharing Approach | • Naval Sea Systems Command (NAVSEA) |
| Innovative Enterprise Decision
Support System | • Office of Naval Research |
| Outstanding Knowledge Expert System | • Virtual Naval Hospital |

Presented at Connecting Technology, Fall 2000

- | | |
|---|--|
| Leading ERP Implementation | • Naval Air Systems Command
(NAVAIR) ERP Team |
| First Successful Reverse Auction
in the Government | • Naval Supply Systems Command
(NAVSUP) NAVICP Team |
| KCO Implementation Effort | • SPAWAR/SSC Charleston Team |
| Creation of the Navy Logistics
Knowledge Portal | • Deputy Chief of Naval Operations
(Fleet Readiness and Logistics)
Portal Team |
| Development of the DoD TOC Portal | • Total Ownership Cost Knowledge
Share Space (TKSS) |
| Digital Dashboard Initiative | • Headquarters, Marine Corps Forces
Pacific

Headquarters, Marine Corps,
Strategic Initiative Group,
Plans, Policies and Operations |



DON eGovernment Awards

Award Category

Award Recipient

Presented at Connecting Technology, Spring 2001

- | | |
|--|---|
| Leading Implementation of eBusiness in the Department of the Navy | • eBusiness Operations Office |
| Outstanding Approach to Developing Knowledge Sharing Networks | • NAVSEA Carrier Maintenance Team |
| Development of a Cross-Service Web-Based Shared Data Warehouse | • NAVSEA PPAIS Development Team |
| Development of a Distributed Interactive Meteorological and Oceanographic Knowledge System | • Fleet Numerical METCAST Team |
| Enterprise-Wide Deployment of the Navy Training Management and Planning System | • Chief of Naval Education and Training (CNET) NTMPS Development Team |
| Outstanding Knowledge Sharing through Communities of Practice | • Naval Facilities Engineering Command (NAVFAC) |
| Outstanding Knowledge Sharing Across the Services | • Major Dale Long, USAF |

Presented at the DON eBusiness Knowledge Fair, August 2001

- | | |
|---|---|
| Leveraging and Sharing Business Solutions | • Commander-in-Chief, U. S. Pacific Fleet Solution Facilitator Initiative Team |
| Implementing a World Class eBusiness Solution | • Naval Medical Information Management Center DENCAS Team
Department of the Navy Smart Card Office DENCAS Team |
| Outstanding Warfighter Support | • Naval Sea Systems Command Distance Support Team |
| Providing Web-Based Tools for Knowledge Management | • Chief of Naval Operations (OPNAV N40 and OPNAV 09B) HQWeb Team |
| Operationalizing Knowledge Management Concepts | • Naval War College, Wargaming Department, Global War Game KM/IT Team |
| Innovative eBusiness Strategies | • NAVSEA Seaport Team |
| Leading Development of the DON's Integrated Supply System | • NAVSUP One Touch System Team |
| Shipboard Collaboration and Knowledge Management | • SPAWAR WeCAN Project Team |
| Excellence in Collaboration Innovation | • Capable Warrior Team of the Marine Corps Combat Development Command Warfighting Lab |



DON eGovernment Awards

Award Recipients

Presented at Connecting Technology, Spring 2002

- NAVAIR Engineering Investigation Business Process Reengineering Team
- USMC Legacy Applications Team
- CNET Electronic Training Jacket Team
- NAVSEA Keyport Division Knowledge Integration Toolkit Team
- GATOR Link eBusiness Pilot Project Team—
Advanced Amphibious Assault Vehicle Program
DON eBusiness Operations Office
- Deployment Logistics Program Team—
Naval Regional Contracting Center, Naples
DON eBusiness Operations Office
- Medical Appointments on the Web Pilot Project Team—
Naval Medical Center, San Diego
DON eBusiness Operations Office

COMMUNICATIONS AND OUTREACH



The DON conferences and awards, and the connections they make across the Enterprise, are part of an aggressive communications and outreach program that focuses on sharing the tools and initiatives generated by the Department. The Clinger-Cohen Act (CCA) points out the need for sharing knowledge and reducing duplication in order to become more effective and efficient in achieving mission goals. Rather than individually addressing problems and producing multiple, redundant solutions, the CCA encourages working together as an Enterprise to produce common solutions to common (Enterprise-wide) problems. The DON Communications and Outreach program responds to the CCA by establishing communities, sponsoring events, publishing information, and providing learning and growth opportunities on IT-related issues and initiatives. Using a multilayered approach, the program provides outreach services and tools to Navy, Marine Corps, and Civilian personnel, and our industry support team, on issues that exist across the Department.

The Communications and Outreach Team consists of a group of people whose skills include public relations, writing and editing, graphic design, video production, and Web design. The Communications and Outreach approach supports the DON CIO's multilayered knowledge sharing strategy, defined in Chapter 9, "Managing Change." Figure 3-3 illustrates the Communications and Outreach Team's role. The following are a few examples of the DON change strategy and how the Communications and Outreach Team supports that strategy.

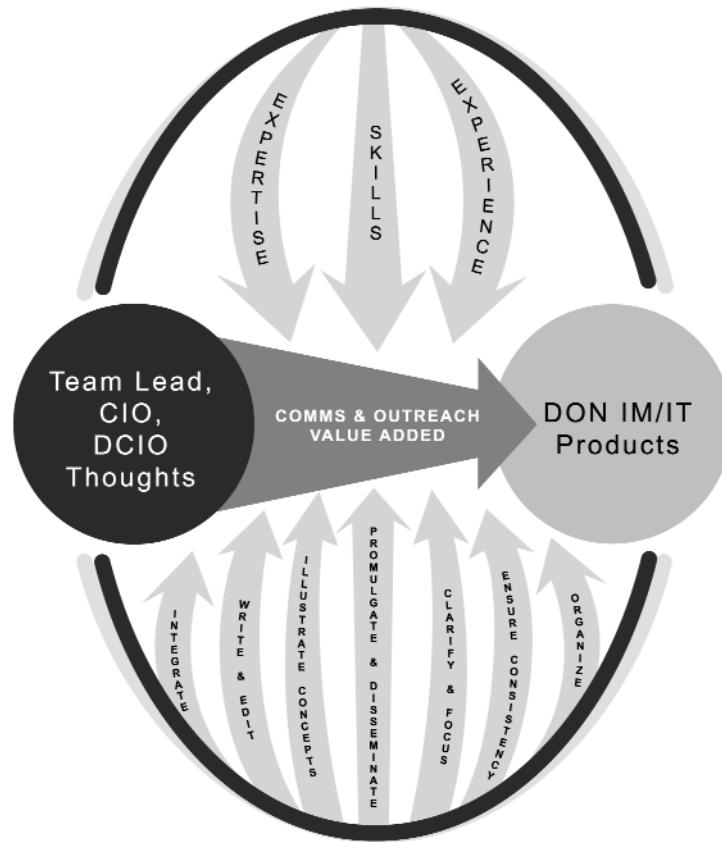


Figure 3-3—DON CIO Communications and Outreach Team Role

Demonstrate leadership commitment. As champions for IM/IT initiatives emerge across the Department, the Communications and Outreach Team captures these leaders on videotape, sharing their ideas, concepts, and commitment to IM/IT initiatives, strategically placing this information on its CDs and written products for distribution.

Facilitate a common understanding. Words and visuals are the tools of trade for developing a shared understanding of IM/IT initiatives. Through the use of articles, presentations, and graphics, the Communications and Outreach Team assists in facilitating a common understanding of emerging IM/IT concepts.

Set limits. By publishing articles in the DON's quarterly IT Magazine, and sending a virtual newsletter to the DON IM/IT community, the Communications and Outreach Team helps to provide the focus, thereby setting limits to facilitate deeper understanding of IM/IT concepts, and the creation of new ideas in these areas.

Provide tools. Using their experience and skills to add value to the ideas and concepts of the DON team leaders for IM/IT initiatives, the Communications and Outreach Team produces the tools that provide approaches to and resources for accomplishing the guidance and policy set forth by the DON CIO. A collage of tools developed by the DON CIO and distributed across the Enterprise is provided as Figure 3-4.

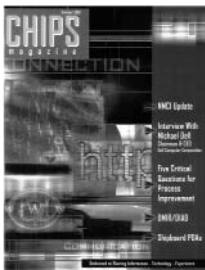


The IM/IT tools that the DON CIO develops improve the efficiency and effectiveness of DON programs. These tools, which are developed for use by the entire Department, and shared across government and with our industry and academia partners, include: the DON IT Capital Planning Guide, the IT Investment Practices Portfolio Model, the DON Integrated Architecture Database CD, DON XML Developer's Guide, Data Management and Interoperability Repository (DMIR), the Knowledge-Centric Organization Toolkit CD, the cPort Communities of Practice CD (in partnership with the Federal Aviation Administration), the Information Literacy CD, the CIP Self Assessment Tool CD, Privacy CD, Learning in a Virtual World CD, the Workforce CD and a special KM Working Group CD (in partnership with the Federal CIO Council). These tools are distributed at fairs, symposia, and meetings, and are also highlighted at one-day tools workshops. These workshops are designed to provide IT management in-depth knowledge of available IM/IT tools that are (1) developed or piloted by the DON, (2) championed by DON users, (3) directly related to the DON IM/IT Strategic Plan, (4) in support of the CCA, and (5) provide solutions for leveraging investments and avoiding duplication.



The DON CIO-sponsored Web site (www.don-imit.navy.mil) facilitates effective information flow about IM/IT issues and initiatives in the DON. The Web site encourages open communications throughout the Department by providing a source of information and a forum for information exchange. The Web site contains content areas for all current DON IM/IT initiatives and interest areas, news, hot topics, reading picks, IM/IT planning and budgeting tools, user forum areas, and user feedback.

The *InfoAlert* newsletter is a communications vehicle that informs the DON IM/IT community of important and timely items of interest, issues, and technology related to IM and IT affecting the DON. Issued two to three times per month, as items of interest become known, each *InfoAlert* is sent via e-mail to a database of over 1,000 recipients, and is posted to the DON IM/IT Web site.



CHIPS magazine is another vehicle used by the DON CIO for connecting across the Enterprise. *CHIPS* is the DON's quarterly IT publication dedicated to sharing technology, information, and experience. *CHIPS* brings timely and thought-provoking ideas to the IT community to stimulate thought, discussion, and exchange. *CHIPS* features a message from the DON CIO, policy and program articles by top DON and DoD program managers, lessons learned from afloat and ashore commands, and the latest technology innovations.

In addition to sponsoring and contributing to each issue of *CHIPS* magazine, the DON regularly publishes articles in journals that are distributed to a worldwide readership. Articles and papers written by DON leaders have also appeared in *Knowledge Directions*—the Journal of the Institute for Knowledge Management; the *Journal for the American Productivity and Quality Center*; *Knowledge and Innovation*; and *Knowledge Management* magazine. The DON CIO also worked with the eGovernment organization to edit two books on KM in government with profits going to the Navy Relief Society.



Figure 3-4—DON IM/IT Tools

Interviews with the CIO, Deputy CIOs, and team leaders appear in various Federal weekly newspapers, including *Government Computer News*, *Federal Computer Week*, *Computer World*, *CIO Magazine*, *Navy Times*, *Federal Times*, *Inside the Navy*, *Defense News*, and numerous others.

In its efforts to connect across all levels of the Enterprise, DON CIO sponsors conferences aimed not only at the IT professional and IT manager, but also sponsors the CIO Executive Symposia—one-day educational and networking opportunities for CIOs throughout the DON community. Participants gain perspectives on current IT issues and insights into the many DON initiatives focused on Enterprise solutions. The emphasis is on showing the critical importance of IT and IM as the key enablers for improving organizational performance. This is a forum where CIOs hear and discuss common issues and share knowledge on best business practices and lessons learned. Symposia topics include subject areas endorsed by the Federal CIO Council as essential for complying with the CCA.

CONCLUDING THOUGHTS



The DON is a large government enterprise consisting of about 800,000 Civilian and Military personnel and interacting with millions of government and industry partners worldwide. The strategies employed for connecting this vast Enterprise directly contribute to the effectiveness of the DON. While IT is our greatest enabler, people are our greatest resource. Ultimately, the role of all of our technology, information, and knowledge resources is to enable decision-makers at every level—at home and abroad—to make the best possible decisions aligned with the Naval mission.

CHAPTER 4

Focus On Governance and Infrastructure

- 4.1 *IT Oversight*
- 4.2 *IT Governance*
- 4.3 *IT Standards*
- 4.4 *IT Infrastructure Architecture*
- 4.5 *Navy Marine Corps Intranet*
- 4.6 *IT Enterprise Architecture*
- 4.7 *Data Management*
- 4.8 *Electromagnetic Spectrum*
- 4.9 *Technology Enablement Strategies*

INTRODUCTION

The importance of a standardized information technology (IT) architecture across the Department of the Navy (DON) can be illustrated by the Winchester Mystery House in San Jose, CA. The house was innovative, but complex, redundant, and costly. Begun in 1884 for Sarah L. Winchester, heiress to the Winchester Fortune, the house was built over 38 years at a total cost of \$550,000 (\$165 million in today's dollars). The house (shown in Figure 4-1) has 160 rooms, 40 bedrooms, 47 fireplaces, 40 staircases, 950 doors, and 10,000 windows. The best builders were hired. Leading edge innovations abound—wool wall insulation, gas lights, intercoms, water recycling, automated watering systems, a no clog sink, and the house has three patents for its innovative design aspects. While there were 147 master builders, there were no architects, no blueprints, and no master plan. Consequently, there are 65 doors that lead to nowhere, 2 basements, 24 skylights in floors, 13 staircases that dead end, and a chimney that rises four stories from the basement, stopping two feet short of the roof. The house is heated by steam, forced air, gas fireplaces, wood fireplaces, and coal fireplaces.

When the Chief Information Officer (CIO) adventure first started, the DON CIO laid out a roadmap to success in the IT infrastructure area with the intent of avoiding unnecessary complexity, redundancy, and excessive cost—in short, optimizing IT at the Enterprise level.

In the past, each of the DON Functional Sponsors and their related shore commands helped foster the thought that information technology, information systems, networks, etc. should all be planned, funded, developed, and fielded within each of their respective functional areas or business units (as shown on Figure 4-2). That usually meant that each of the Functional Sponsors would plan and develop systems that performed extremely well within each of their business units, but not necessarily *across* business units. It also created another phenomenon, now commonly referred to as the “digital divide.” Any sponsor (or



Figure 4-1—The Winchester House symbolizes innovation at its best with no shared vision or connectedness of choices.

their related shore command) that could budget for or reprogram sufficient funds to meet their IT needs found ways to keep relatively abreast of new technology. Those that didn't, always lagged behind the 18 month technology cycle by at least two or three generational changes, becoming the IT "have-nots."

The DON CIO looked at the senior staff from the Secretariat, Chief of Naval Operations (CNO), Commandant of the Marine Corps (CMC) and the Operational Forces as being key partners in the Department's IT transformation. It would only be with their direct involvement that the Department would be able to develop a computing and communications infrastructure that could truly become the means for establishing an Enterprise strategy required for DON sustainment and growth in the 21st Century. With their buy-in, the next field of opportunity would be a concerted focus on the Functional and Resource Sponsors.

It was the DON CIO's long-term intent to figure out a way to normalize this phenomenon, making workstations, networks, computing platforms, and applications a core utility the Functional and Resource Sponsors and their shore commands could build on (see Figure 4-3). But, in order to do this DON first needed to establish a means to "govern" IT within the Department. While the Clinger-Cohen Act of 1996, as amended, gave the Department's CIO sweeping accountability and responsibility for IT, the CIO did not control the money used to buy or field IT. With that understanding, the Office of the DON CIO established a Board of Representatives (BOR) made up of all of the Functional and Resource Sponsors and each of the major shore Commands across the Department. This forty person board became the primary advisory group to the DON CIO in its first year following standup. As representatives from the major buying communities, the BOR wanted the newly formed CIO to focus on developing and publishing IT standards that the individual claimants could use when they bought their IT locally to help close the

SECNAV, CNO, CMC, Operational Forces								
Weapons Systems	Intel	C3	Logistics	Training	R&D	Medical	Personnel	Financial
		Functional Requirements & Funding						
			Systems Planning					
			Applications					
			Computer Platforms					
			Networks					
			Workstations					
SECNAV, CNO, CMC, Operational Forces								

Figure 4-2—Pre-CIO. Each functional area optimized IT for its area of business.

Department's interoperability gaps. More information about the BOR and other IT governance structures is contained later in this chapter.

The Department's best and brightest IT people were assembled to form an Integrated Product Team (IPT) which, for eighteen months, labored at developing a set of standards that could be used in any procurement. Since the Department had no overall functioning architecture, the IPT had to focus also on initial development of an IT architecture to help formulate and guide the assumptions used in creation of the Information Technology Standards Guidance (ITSG) document. The ITSG, the DON CIO's first official reference document, became one of the DON CIO's cornerstone documents, later used in the formation of the assumptions for the Global Networked Information Enterprise (GNIE) under development by the Department of Defense.

The ITSG is a continually evolving reference document that changes as new standards emerge. A good example of this is the technical compliance standards set forth in Section 508 of the Rehabilitation Act. Section 508 requires that all Federal agencies ensure that any electronic and information technology (EIT) developed, procured, maintained, or used by the Federal Government is accessible to and usable by all Federal employees and Federal customers with disabilities. This applies to all hardware, software, Web sites, e-mail, video, and multimedia systems, and even ATMs and fare card machines on Department of the Navy property. It also applies to all equipment used for transmitting, receiving, using, or storing information, including telephones, fax machines, copiers, and calculators.

SECNAV, CNO, CMC, Operational Forces								
Weapons Systems	Intel	C3	Logistics	Training	R&D	Medical	Personnel	Financial
		Functional Requirements & Funding						
		Systems Planning						
			Applications					
			Computer Platforms					
			Networks					
			Workstations					
SECNAV, CNO, CMC, Operational Forces								

Figure 4-3—Current IT Reality where workstations, networks, computer platforms and applications are a core utility.

Realizing the shortcomings the IPT faced not having a technical architecture when developing the ITSG, another IPT was formed to develop what became known as the Information Technology Infrastructure Architecture (ITIA). The ITIA was the DON CIO's first integrated architecture product that integrated land-based and shipboard local area networks, wide area connectivity, teleports, and satellite bandwidth requirements. Like the ITSG, the ITIA became a formulation reference document for the Global Networked Information Enterprise.

Even with these attempts at developing and standardizing procurement directions, it was becoming clear that an alternative means of procuring IT would be required if the DON were ever to shift the "have not" imbalance. Historically, DON had budgeted for and operated over one hundred different data and communications networks within the Department. Each of these networks was locally developed, locally procured and maintained, and adhered to local standards and implementation schemes, in spite of the ITSG/ITIA efforts. This situation brought inherent incompatibilities, functional duplications, and restricted adoption of modern network computing techniques that would allow DON to minimize operations and support costs. The most challenging issue was to determine the best acquisition approach.

A number of different procurement and policy based approaches, such as stronger enforcement of the ITSG and ITIA, were considered. Year end funds, or what the

government calls sweep-up funds, had often been the source for many of the Department's PC purchases in the past, as was tapping into appropriated programs for IT and IT support. But these programs could not be the vehicles for providing basic IT computing services. In those years of constantly shrinking Defense procurement program budgets, the Department had to ensure that program funds were being used for their intended purposes. Traditional acquisition approaches fell short because they required large up-front capital investments, estimated at the \$3.5 plus billion dollar level. Even if the DON were able to secure that amount of funding, it would still be continually challenged to find recurring funds to keep up with rapid technology advances made by industry.

The alternative chosen was to adopt the prevailing industry approach which appeared to provide more IT performance at significant cost advantages. Building on first principles of DON Acquisition Reform, such as performance based contracting, and with strong senior Department backing from the Secretary down, the DON CIO laid out a plan to acquire IT capabilities via a fixed price, performance-based services contract. In this manner, IT computing and communications capabilities are consumed and paid for in much the same way that other utilities are purchased. Under the Navy Marine Corps Intranet (NMCI) concept, the Department would formalize its computing and communications requirements across the Department as a managed utility. This innovative approach was not an easy concept to sell—either internally or externally.

With the NMCI effort focusing on a fundamental change in the way the Department procured and operated IT systems, there was the understanding that this had to be a major team effort, with buy-in from the senior levels as it cut across all boundaries, throughout the DON as well as the DoD and Congress. Within the Department, the Secretary, the Under Secretary, Chief of Naval Operations, Commandant of the Marine Corps, Fleet Commanders-in-Chief, and all Echelon II claimant Commanders became personally involved in development of the NMCI concept and its eventual acceptance across the Department. Within DoD, the Office of the Secretary of Defense (OSD) staffs, the Joint Staff, and the Defense Information Systems Agency (DISA) all became partners in the NMCI evolution.

Additionally, with a contract effort approaching the estimated size of \$6.9 billion dollars, the Office of Management and Budget (OMB) and Congress took considerable interest in NMCI. In what would become the largest IT contract ever awarded in the Federal Government, the NMCI team under the Program Executive Office for Information Technology (PEO-IT) had charted a new "procurement waters" course. When it became clear that NMCI could potentially obviate thousands of Civilian and Military IT functions, many of these constituents began writing their Congressman, concerned about the inequities of the Department's NMCI efforts and the fact that the approach was forcing them out of jobs. It took months to convince both Congress—as well as leaders within the Department—that NMCI was not a wholesale "outsourcing" effort. The Department made it clear that it was fully committed to supporting any personnel affected by NMCI as they transitioned to other government jobs within the Department. DON also requested that the potential NMCI vendors add a "personnel parachute" clause in their proposals so that all affected DON Civilian employees who wanted to remain in the affected IT areas could join the winning contractor's team. It should be noted that of the 239 Civilian positions

that were affected by the NMCI implementation during fiscal year 2001, 45 took positions with EDS, the NMCI contractor. There were no involuntary separations.

The DON also spent a great deal of time trying to figure out how NMCI could be used to maintain sea-shore rotation, enhance retention, and improve skill levels for our Military IT personnel. The Navy validated 242 IT billets for reassignment to NMCI. Similarly, the Marine Corps identified 251 Marine positions. While the Service personnel would incur an additional minimum tour commitment after completing a 36 month tour of duty with NMCI, they would receive state-of-the-art, industry standard training as part of their assignment to NMCI, greatly benefiting these Sailors and Marines when they returned to the Fleet.

After much deliberation, the Congress, OMB, and OSD allowed the Department to award the NMCI contract on October 6, 2000. Going back to the original CIO normalization plans as shown in Figure 4-2, NMCI would normalize the workstations, networks, and many of the computing platforms in the Department. It covered a tremendous portion of those original plans, but technology alone, no matter how good or efficient it is, could not solve all of the Department's information systems problems. Without a complete, compelling architecture, the Department would still be lacking the vital roadmap information it needed for 21st Century operations.

While the NMCI contract was under initial development, the DON CIO and BOR chartered a third IPT to focus on data and data management, and its primary facets of data quality, standards, storage, and security. This Data Management and Interoperability (DMI) IPT, made up of data management experts from over 40 Navy and Marine Corps commands, completed a year-long effort focused on defining the policy, processes, and tool requirements to support development of a data architecture. The IPT realized that while the technology side always wins the glitz and glamour contest, the most challenging task for any CIO is applying the time and resources needed for development of an Enterprise-level data architecture that minimizes redundancy, promotes interoperability, and ensures integrity of the data used across the Enterprise. Since data is really the key element exchanged across the DON's organizational and functional boundaries, acceptance and cooperation from the major functional stakeholders (i.e., personnel, finance, acquisition, logistics, intelligence, etc.) would be paramount to the architecture's ultimate success or failure. Thinking positively, completion of the entire Enterprise architecture model will almost finish the transition to a common computing and communications infrastructure. More details on the Department's Enterprise Architecture initiatives are included in Section 4.6. More information on the DMI initiatives is included in Section 4.7.

As technology continually changes, the DON CIO recognizes the positive effects some of these changes could have on the way the Department works. The DON CIO's Technology Enablement Strategies group investigates ways to exploit these emerging information technologies to achieve performance breakthroughs in the way the Department conducts business. Perhaps the most notable of these has been the seeding and rapid adoption of handheld wireless technologies.

For quite some time, personal digital assistants (PDAs) had been an extension of the IT capabilities shared by many DON employees. Many forms of PDAs exist, each with their

own set of unique features. They were normally used to keep track of schedules, synchronize with computers at work, and download e-mails, with the ability to read them and answer them as time permitted—in or out of the office. Of course, users would have to wait to get back into their offices to synchronize with their desktop machines before the e-mails could be sent. When modem cards were introduced into the world of PDAs, people could dial into their networks to send and receive e-mail, expanding their work horizons even further. These mobile devices caused quite an uproar in the security community as they were “walking” possibilities for unsecure access into the Department’s networks. This became of even more concern when serious security holes were found in the 802.11 transmission standards.

One PDA appeared out of nowhere (built around pager technology) that was Federal Information Processing Standards (FIPS) certified from a security standpoint, had triple Data Encryption Standard (DES) encryption, and offered a serious remote e-mail capability people had not quite envisioned yet. Under the DON CIO’s direction, the Technology Enablement Strategies group investigated and started to seed these devices with senior management across the Department. The devices offered an “always on” capability, 24 hours a day no matter where they were located, depending on wireless coverage.

The IT infrastructure products discussed in this section provide the critical underpinnings required for the health and growth of the IT economy across the Department of the Navy. In effect, without these products, the DON would never be able to achieve the transformational changes envisioned by the leadership of the Department.

4.1 IT Oversight

The architects of the Clinger-Cohen Act had the wisdom to recognize historic inefficiencies in the procurement of IT resources. It is now incumbent upon us to embrace that foresight and implement a management philosophy that will result in world-class Navy IT systems being deployed with a high degree of efficacy.

—John J. Lussier, CCA Implementation and Compliance Team Leader

BACKGROUND

The Clinger-Cohen Act (CCA) positioned Federal Government acquisition of information technology (IT) at the forefront of Congressional oversight, and empowered the executive branch to establish an effective Federal IT infrastructure. The passage of the Clinger-Cohen Act gave recognition to the ever-increasing reliance on IT for management of many Federal Government functions, along with the requisite to acquire assets based on their capacity to enhance delivery of services. The Clinger-Cohen Act represents a statutory response to historic inefficiencies in the procurement of information technology resources. The 1994 “Computer Chaos” report released by Senator William Cohen of Maine highlighted some of the difficulties the Clinger-Cohen Act is intended to resolve. As provided in Chapter 1 these are:

- Insufficient use of business processes in determining an appropriate investment strategy for IT.
- Prior IT investments made by Federal agencies that neither improved mission performance nor satisfied their original intent.
- Implementation of ineffective information systems resulting in waste, fraud and abuse.
- Antiquated IT procurement strategies that did not adequately address the competitive and rapid life cycles market forces associated with industry IT products.

The Clinger-Cohen Act also helped the Department of the Navy (DON), like all Federal agencies, to focus energy on interoperability and the implementation of a program to ensure that adequate security is provided for all information collected, processed, transmitted, stored, or disseminated. Figure 4.1-1 demonstrates the criticality of both interoperability as well as information security. Toward this end, and to address the previously mentioned difficulties, one of the DON Chief Information Officer’s (CIO’s) primary responsibilities under the Clinger-Cohen Act is to oversee investments in IT, including National Security Systems (NSS), to ensure that the Department’s IT systems are interoperable, secure, properly justified, and contribute to mission goals.

LEGISLATIVE AND REGULATORY IMPLEMENTATION

The DON CIO is the Navy's authority and point of contact for policy and procedures related to the Clinger-Cohen Act. Relative to IT program oversight, the function of the DON CIO in carrying out the intent of the Clinger-Cohen Act is focused primarily on:

- Providing policy, guidance, and assistance to component CIOs, program managers, and information technology professionals throughout the Department of the Navy.
- Confirming or certifying that mission critical and mission essential information technology systems are being developed in accordance with the Clinger-Cohen Act's intent.

Policy directive DoD Instruction 5000.2 requires that programs designated as Major Automated Information Systems (MAIS) have a certification of compliance approved prior to award of a contract. Further, DoD Instruction 5000.2 requires that the Milestone Decision Authority not approve program initiation or entry into any phase that requires milestone approval until certification of compliance with the Clinger-Cohen Act is approved. This directive includes acquisition of mission-critical or mission essential IT programs, including NSS. Certification of compliance entails a review and recommendation by the DON CIO, with formal approval obtained from the DoD CIO.

Confirmation of compliance with the Clinger-Cohen Act is made by the DON CIO for all other acquisition category programs, with no formal approval required of the DoD CIO.

Because of the fact that IT is pervasive throughout all modern Navy systems, and specifically because NSS are identified as being subject to the CCA, there was concern that certain types of acquisition programs (e.g., weapons systems, platforms, etc.) would be subjected to duplicative and redundant reporting requirements. These types of acquisition programs already have a very robust set of requirements for reporting as part of their normal acquisition process.



In an effort to help ameliorate duplicative reporting requirements, the DON CIO took the lead and collaborated with the Office of General Counsel, DoD CIO and other Services to amend the DoD instruction regarding CCA compliance for IT systems that are an integral part of, or contained in, a weapons system or platform (e.g., ship, aircraft, or tank) and IT systems used for command and control. The modifications to the regulations allow program managers to cross-reference to the already existing acquisition documentation to address the CCA requirements, and for the judicious application of the other requirements of CCA "to the extent practicable." This greatly reduces the administrative burden on the program management community, and eliminates the non-value added requirements.

DON CIO support to Department program managers is evident under three process domains: IT Systems Registration, CCA Confirmation, and CCA Certification. For each of these domains, an online, automated support tool has been developed by the DON CIO and is available at www.don-imit.navy.mil. These Web-based tools provide guidance, instruction, and the capability to complete the reporting requirements online. Additionally,

the Web site contains bulletin boards to provide information relative to upcoming events sponsored by the DON CIO, DON policy statements and directives, information alerts, and news pertinent to Federal policy and guidance for acquisition of IT.

IT SYSTEMS REGISTRATION

Sections 8102 and 811 of the Fiscal Year 2001 DoD Appropriations and Authorization Acts, respectively, require that all mission essential and mission critical IT systems be registered with the DoD CIO.



In order to accomplish this, the DON CIO has developed a Web-based database using the security for Sensitive But Unclassified (SBU), supported by Public Key Infrastructure (PKI). Data security is of primary concern, as the information contained within the data fields summarizes a significant portion of applications managed by the DON. A user can authenticate to the database either by personal DoD certificate or by name password in the event they do not have a certificate. Access control is provided down to the file level where required.

The IT Registration Database contains all Navy computer systems and supports Office of the Secretary of Defense/Congressional data calls. This enables IT system managers to update their records securely from anywhere in the world that has an Internet connection, meeting all requirements necessary to protect SBU information. The data management challenges include:

- Centralizing, coordinating, and maintaining IT systems data.
- Ensuring ease of use and reporting for accurate real-time analysis.
- Supporting continued preparation of strategy for post-IT Systems Registration activities, data use, and program integration.
- Supporting immediate information requests.
- Ensuring that US Navy and Marine Corps data is secure.

System owners and major claimants can gain access to the database anytime through the DON IM/IT Web site to register their IT systems and run reports. Users can save their IT systems reports online, or download the file to their desktops for printing, or to use the data for any number of management purposes.

The database is located on the DON IM/IT Web site at www.don-imit.navy.mil/cca/registration. The online tool provides assistance for registering systems, including guidance on what systems should be registered, data fields to be provided, and assistance on how systems should be identified.

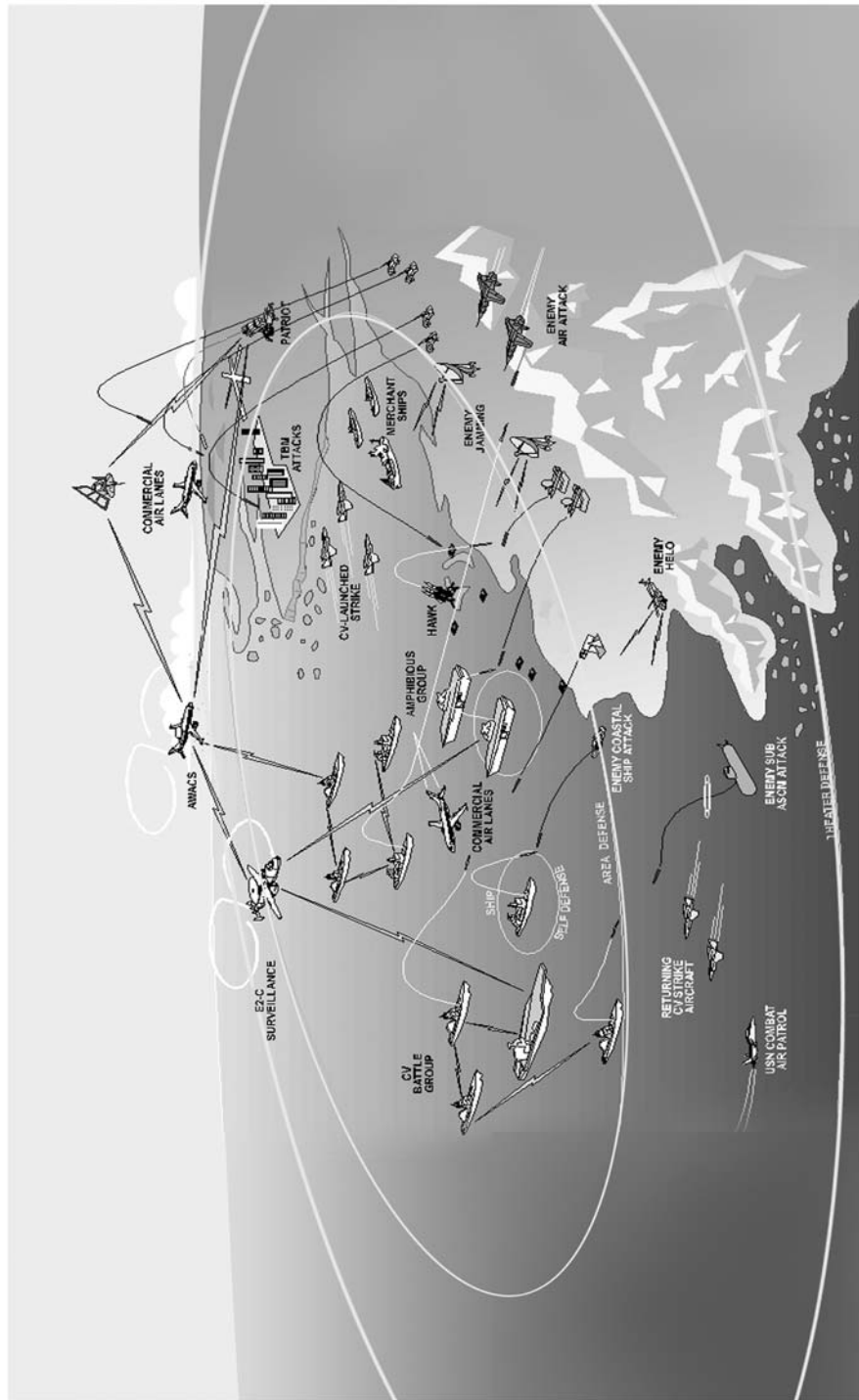


Figure 4.1-1—Both interoperability and information security are critical to success of the DON mission.

CCA CERTIFICATION REPORTING

Sections 8102 and 811 of the Fiscal Year 2001 DoD Appropriations and Authorization Acts, respectively, also require that all Major Automated Information Systems prepare Clinger-Cohen Act Certification Reports prior to milestone decisions and award of major IT contracts. The DON CIO collaborated with the DoD CIO and the other Services to develop a robust Clinger-Cohen Certification template which is also located on the DON CIO Web site at www.don-imit.navy.mil/cca/certification.

The Clinger-Cohen Certification Report template is an automated tool that provides Program Managers (PMs) a template and amplifying guidance, complete with links to reference materials, source legislation, directives, examples of good CCA Reports, context sensitive help, subject matter experts, and further guidance which will assist program managers of IT programs in developing certification reports demonstrating compliance with the Clinger-Cohen Act. Users can develop and save their CCA Certification Reports online, and download the file in Word format to their desktop for final editing, graphics, printing, and signature.

The DON CIO reviews and signs the CCA Certification Reports, and forwards them to the DoD CIO, which has the responsibility to certify to the Congressional defense committees that the program is being acquired in accordance with the Clinger-Cohen Act.

The DON CIO works with component CIOs, PMs, and other information technology professionals toward improving acquisition processes and ultimately obtaining certification for acquisition programs. As IT programs progress through the CCA process, lessons learned and enhanced reporting tools will be added to the Web site.

CCA CONFIRMATION OF COMPLIANCE

DoD Instruction 5000.2 requires that the DoD not award a contract for acquisition of a mission-critical or mission essential IT system until the service CIO confirms that the system is being developed in accordance with the Clinger-Cohen Act. It also requires that the Milestone Decision Authority not approve program initiation or entry into any phase that requires milestone approval for an acquisition program for a mission-critical or mission essential IT system until the service CIO confirms that the system is being developed in accordance with the Clinger-Cohen Act.

Demonstration of Clinger-Cohen Act compliance for confirmation purposes may be in the form of briefing materials, a set of existing documents (such as acquisition milestone documents), a single document summarizing the required information and pointing to other detailed sources, or other appropriate documents. The DON CIO reviews the compliance information and makes a determination of Clinger-Cohen compliance, providing a written confirmation to the DoD CIO and the Milestone Decision Authority.

To assist PMs in development of Clinger-Cohen confirmation information, the DON CIO has developed an automated, Web-based confirmation template. This template provides an outline and resources for completion of the confirmation process. There are links to source legislation, directives, and further guidance to complete a confirmation report demonstrating compliance with the Clinger-Cohen Act.

4.2 IT Governance

One of the most difficult challenges facing the Federal, DoD and DON IT communities in the 21st Century is the governance of Information Technology. The reason that this challenge is difficult is the diverse nature of local commands, the wide variety of IT requirements, and the large number of IT products available.

—Dale Christensen, Strategic Planning and Policy Integration Team Leader

BACKGROUND

Similarities can be found between the early history of our country and the Department's governance of information technology (IT). *The Federalist Papers*—a series of 85 essays written by Alexander Hamilton, John Jay, and James Madison between October 1787 and May 1788—were circulated to urge citizens to ratify the proposed Constitution of the United States. These papers provided the underlying thinking of the articles of confederation, focusing on the migration from a form of highly decentralized government to a federation. *The Federalist Papers* argued that with the (then) existing decentralized government, measures would “too often be decided according to their probable effect, not on the national prosperity and happiness, but on the prejudices, interests, and pursuits of the governments and people of the individual States.” In admonishing citizens to adopt a standard coinage, the papers argued that “a right of coinage in the particular States could have no other effect than to multiply expensive mints and diversify the forms and weights of the circulating pieces.” Similar to decentralized government, IT governance at the local command level leads to (1) adoption of IT solutions that benefit the local commands, but not the entire Enterprise; (2) duplication of functions just for diversity's sake; (3) non standard systems; and (4) the lack of interoperability.

Recognizing the consequences of non-centralized IT governance, there has been a flurry of statutory, regulatory, and other guidance in IT over the last five years. It started in 1996 with the passage of the Information Technology Management Reform Act (ITMRA)/Clinger-Cohen Act (CCA) (see Chapter 1, “The Congressional Mandate”) and has continued with Presidential Executive Orders, Office of Management and Budget (OMB) memoranda, Department of Defense (DoD) directives, instructions, handbooks, and DoD IT guidance and policy memorandums, as well as Department of the Navy (DON) policy memoranda. The increased focus on IT is needed, because IT touches almost every segment of the DON warfighter and business functions and processes, and directly impacts mission accomplishment.

The governance of IT is critical since it encompasses the framework, policies, and methodologies that determine how IT systems and infrastructure are designed, developed, implemented, and maintained throughout the DON. It is the key integrating piece that enables systems interoperability and the accomplishment of mission requirements. The challenge of IT governance is the independent nature of the various organizations within

the DON, the wide variety of requirements, and the large number of IT products available. Balancing Enterprise needs with the requirements and products available is a very difficult challenge.

The key players in IT Governance within the DON are the DON Chief Information Officer (CIO), Navy CIO (N6), and the Marine Corps CIO (C4). There are also a number of important DON committees and councils associated with IT Governance. They include: DON Information Leadership Council (DON ILC), DON Information Executive Committee (DON IEC), NMCI Action Group, NMCI Stakeholders' Council, and the Enterprise Action Groups. The key players in IT Governance external to the DON are the OMB Associate Director for IT and eGovernment and the DoD CIO. The key external councils and boards are the Federal CIO Council and DoD CIO Executive Board.

GOVERNANCE BODIES

Federal CIO Council

The Federal CIO Council, the primary government-wide IT council, was established by Executive Order on July 16, 1996. Its charter was approved on February 20, 1997. The CIO Council is the principal interagency forum to improve agency practices for the management of information technology. The CIO Council serves as a forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources. The CIO Council communicates its findings to OMB and other executive agencies. The Federal CIO Council charter also details policy, lessons learned, sponsorship, IT workforce, feedback, and collaboration roles. The Federal CIO Council charter contains the council vision, membership, and other key items. It is available at the Federal CIO Council Web site at www.cio.gov.

DoD CIO Executive Board

The DoD CIO Executive Board (ExecBd) is the principal DoD forum to advise the DoD CIO on the full range of matters pertaining to CCA, as amended, and the Global Information Grid (GIG). The ExecBd also exchanges pertinent information and discusses issues regarding development of the Global Information Grid, including DoD information management (IM) and IT. The ExecBd charter details the policy, GIG, architecture, interoperability, information assurance, capital planning, acquisition, financial, and requirements roles. The ExecBd charter details the roles, responsibilities, and membership and is available on the ASD(C3I) Web site at www.c3i.osd.mil.

DON Information Leadership Council

The DON ILC is the corporate level board to advise and support the Secretary of the Navy on information systems resource planning, content, standardization, investment, funding, management, and the migration to Web-based applications within the DON. The

ILC is chaired by the Under Secretary of the Navy with the Vice Chief of Naval Operations (VCNO) and the Assistant Commandant of the Marine Corps (ACMC) as members. The DON CIO serves as the Executive Secretary. The Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RD&A)) and the ASN Financial Management (FM) may also be invited to provide information or expertise to assist in the deliberations, as necessary. Unresolved departmental IT or NMCI policy, resource, operational or technical issues are forwarded from the DON IEC to the DON ILC for resolution. The DON ILC meets on an as required basis.

DON Information Executive Committee

The DON IEC is the senior level forum for the resolution of information technology issues. DON CIO chairs the DON IEC and members include the Director, Space, Information Warfare, Command and Control, Office of the Chief of Naval Operations (N6/USN CIO); and the Director, Command, Control, Communication, and Computer, Headquarters Marine Corps (USMC CIO). The Deputy Assistant Secretary of the Navy (Command, Control, Communications, Computers, Intelligence, Electronic Warfare, and Space) (DASN(C4I/EW/SPACE)); the Director, Office of Budget and Fiscal Management (FMB); and the Program Executive Officer for Information Technology (PEO-IT) participate as requested. The DON IEC meets monthly, and its primary focus is on IT policy issues and IT strategic direction.

NMCI Action Group

The NMCI Action Group was established in November 2001, to focus on NMCI planning, policy, and implementation issues. The DON CIO chairs the NMCI Action Group and members include the Navy CIO and Marine Corps CIO. The DASN(C4I/EW/SPACE), FMB, and PEO-IT may be included. The Commander Naval Networking and Operations Command and the NMCI contractor are also invited regularly to participate in the NMCI Action Group. The NMCI Action Group meets weekly and its primary focus is on NMCI planning, policy and implementation issues.

DON CIO



The position of the DON CIO has evolved over the past four years as the provisions of the CCA have been implemented. One of the complicating factors within the DON is that there are two separate Services—the Navy and the Marine Corps—each with a different set of cultures and standard operating procedures. This creates additional challenges for the DON CIO to set policy and strategic direction across two very different Military organizations. The DON CIO has been successful by bringing the Navy and Marine Corps CIOs into all major decisions and issues through the use of the DON IEC, NMCI Action Group, integrated product teams, and specific, focused meetings.



While the DON CIO has focused on many different IT areas, it has done so with the focus of helping all personnel within the DON realize that the Enterprise truly is the entire Department, not an activity, not one of the Fleets, nor a Systems Command. The DON CIO has crafted strategies, policies, and approaches that bring all stakeholders together to resolve issues. A good example of this is the NMCI governance process detailed in Figure 4.2-1. The NMCI Stakeholders' Council is the clearinghouse for all significant NMCI issues. All stakeholders have a seat and any can raise an issue. Underneath the Stakeholders' Council are the Enterprise Action Groups (EAGs). When an issue is raised by a stakeholder, it is normally referred to the appropriate EAG. The EAG is composed of major stakeholders and those who own the issue. A resolution is proposed and brought back to the Stakeholders' Council for agreement. If the issue deals with IT policy or strategic direction, it is then referred to the DON IEC for approval. This open process has helped all realize that they are part of the DON Enterprise and all are given a voice.

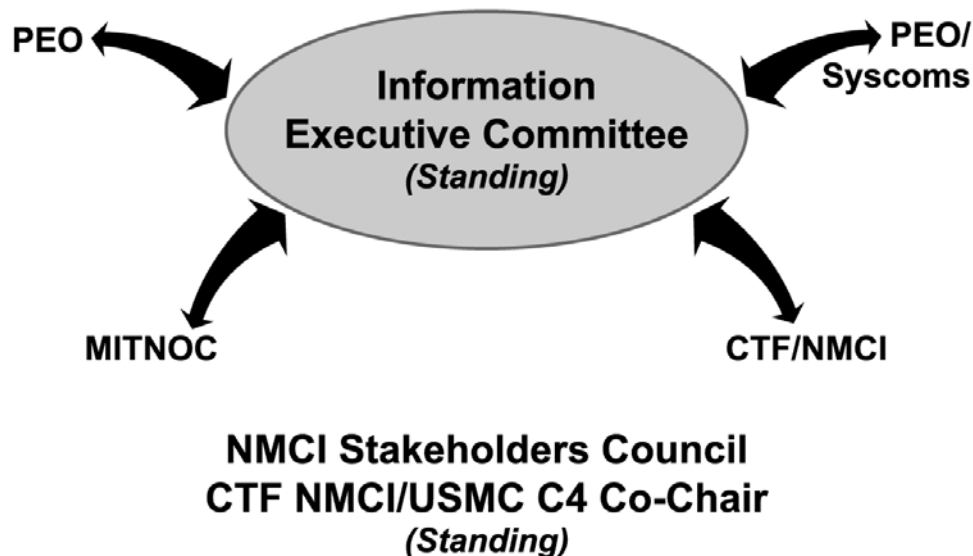


Figure 4.2-1—The NMCI Governance process brings all Stakeholders together to resolve issues.



The DON CIO's Enterprise view of IT is embodied in the establishment of the DON ILC and the DON IEC. With the establishment of the DON ILC and DON IEC, the senior leadership of the Department (the Under Secretary, VCNO, and ACMC) are now involved in issues that are not resolved at the DON IEC level or are outside the scope of the IT community. The ILC has been very supportive and helpful in clarifying the position of senior DON management on major IT issues. One example of a major issue where the ILC weighed in was with the management of software applications. DON policy calls for the elimination of duplicative, obsolete, and non-secure applications and their associated databases. ILC support was critical in furthering this policy, and letting all know the position of senior DON leadership.

Another example of bringing the Enterprise together is the analysis done by the DON CIO on the Governance councils, committees, and groups. It became apparent that some changes needed to be made in managing the Enterprise Resource Planning (ERP) pilots. Using the DON ILC as the approving body, a relationship was created between the ERP, Executive Steering Group, and the DON IEC to facilitate the “Enterprise” aspect of ERPs.

CONCLUDING THOUGHTS

The bottom line philosophy here is that everyone needs to have a seat at the table, that problems and issues are resolved through collaboration, and that there is a shared power structure.

As the role of IT continues to grow within the DON, IT Governance becomes more important as well. The DON CIO plays a pivotal role along with DoD, Navy, and Marine Corps CIOs, as well as the CIO boards and councils at the government-wide, DoD, and DON levels. The DON CIO has led the way—and will continue to lead the way—by using both the internal and external CIO bodies as collaborative forums to further IT Governance and the effective design, development, implementation, and maintenance of DON IT systems and infrastructure.

4.3 IT Standards

The establishment of IT Standards is critical to the evolution of an interoperable Enterprise IT infrastructure.

—Tom Scruggs, Computing and Communications Infrastructure Team Leader

BACKGROUND

Back in the mid-1990s, the General Accounting Office (GAO) published a widely acclaimed study known as the *11 Best Practices for Information Technology (IT)*. An alarming percentage of organizations implementing IT were failing, particularly in government. GAO found that, in industry and government organizations that had successfully implemented IT programs, there were 11 best practices consistently and commonly employed. One of the most important of these was a defined and accepted set of IT architecture and standards. The tenets of the “Best Practices” were the foundation for the Clinger-Cohen Act of 1996, which in turn was the genesis of the Office of Management and Budget Memorandum 97-16, Information Technology Architectures (ITA). The ITA requires the DON CIO to develop, maintain, and facilitate implementation of the Department’s information technology architecture and standards. The development of IT standards was the first area of opportunity on which the newly formed Office of the DON CIO was asked to focus its attention.

DESCRIPTION



The DON Information Technology Standards Guidance (ITSG) was written by an Integrated Product Team (IPT) of subject matter experts from across the Department. The ITSG identifies and describes IT specifications, standards, products, and best practices for the DON, based on the criteria of security, functionality, interoperability, performance, and cost. A feature throughout the ITSG is the depiction of the recommended, emerging, and not recommended standards or technologies to be used by all of the Navy and Marine Corps IT managers for consistent IT planning, development, and implementation.



The ITSG was considered absolutely essential by the DON CIO’s Board of Representatives since the original acquisition strategies revolved around multiple, decentralized implementations that had to be complementary and interoperable. The most visible example of this is the ITSG’s series of “continuum” charts, illustrated in Figure 4.3-1, that identify the current standards, the projected standards, the emerging standards, and the not-recommended standards. This allows planners, implementers, and acquisition personnel to anticipate changes in standards and specifications, and thereby, multiple DON organizations that are implementing networks in a decentralized fashion can be successful.

	Current ITSG	Projected ITSG			
Not Recommended	1999	2000	2001/ 2002	2003/ 2004	Emerging
Selecting any of these specifications, products, or technologies is not recommended.	Select specifications, products, or technologies based on this time line.				These specifications, products, or technologies are being monitored as potentially significant.
Activities, Platforms, Operational Environments		The specifications, products or technologies above apply to these platforms or operational environments.			

Figure 4.3-1—ITSG continuum charts identify the current standards, the projected standards, the emerging standards, and non-recommended standards.



The development of the ITSG prior to the development of an IT Information Architecture (ITIA) resulted in temporary overlaps in the type of information presented in each document. Information about the ITIA is presented later in this chapter. Now that the ITSG has been published, some of the process and service descriptions that are more architecture oriented will be removed from upcoming revisions. To use a town planning analogy, the purpose of the ITSG was to provide the building codes to detail the specific interfaces and products that should be used. The intent for the ITIA was to describe the way the building design and services address required customer functionality. This alignment of information will be performed during subsequent updates of the two documents.

The ITSG's scope is all IT. Therefore, only a subset of the ITSG is directly applicable to the ITIA, whose scope is limited to the common infrastructure (including the network and network services) upon which applications run.

IMPLEMENTATION



The actual ITSG development process was fraught with challenges. Establishing the right membership on the team was critical since it was necessary to achieve balance between multiple competing objectives. These objectives included organizational unit representation to facilitate the following while still keeping the team small enough to be effective:

- Eventual Enterprise-wide acceptance of the guidance.
- Representation by true subject matter experts (regardless of organizational affiliation) for the many functional areas addressed by the document.
- Representation by people who could put their “best for the Enterprise” hat on vice their “best for my organizational unit” hat.

As with any complex team effort, having the “right people on the bus” was the key to success.

Because the scope of the ITSG is the entire realm of IT, the initial release did not cover the entire breadth and depth that will eventually be in the document. Also, because of the rapid evolution of IT, the document becomes stale fairly quickly, and, due to the subsequent development of closely related products such as the ITIA and the NMCI effort, described later in the chapter, some modifications to the ITSG have become appropriate. The DON CIO has embarked on an effort to expand and update the ITSG and then iteratively co-evolve the ITSG with other related DON CIO products.

Upon completion of the ITSG, the draft document was vetted throughout the Department. After a lengthy review, the final product was unanimously approved by the DON CIO Board of Representatives and became the first deliverable of the DON CIO. Having an IT Standards Guidance document provided the building codes that could be used by the Department’s IT infrastructure planners. Armed with the ITSG and confidence in the power of properly constructed DON Enterprise-wide teams, the DON CIO Board of Representatives chartered the ITIA IPT to take the next step on our journey. As you will see, this too was a very successful team effort.

4.4 IT Infrastructure Architecture

The IT Infrastructure Architecture Plan served as the foundation for the performance, layered security, and consolidation/integration strategy of the Department's Navy Marine Corps Intranet and the Department of Defense Global Information Grid.

—Tom Scruggs, Computing and Communications Infrastructure Team Leader

BACKGROUND

During development of the Information Technology Standards Guidance (ITSG), it became apparent that we needed to make some architectural assumptions since the DON did not have an IT infrastructure architecture. This recognition led to the decision by the DON CIO Board of Representatives to charter development of a DON Information Technology Infrastructure Architecture using the same integrated product team (IPT) approach that was so successful during development of the ITSG.

DESCRIPTION



The DON Information Technology Infrastructure Architecture (ITIA) was written by a 40 member Navy and Marine Corps IPT of subject matter experts. The ITIA describes the manner in which information will be exchanged over networks at the wide area, the metropolitan area and the campus area. The complex document defines the IT infrastructure components, identifies demarcations, selects protocols, describes network services, suggests best practices, establishes performance metrics, and states how security mechanisms will be employed. ✓

The ITIA successfully developed a solution path by acknowledging the multitude of legacy physical networks in the DON that must be accommodated, and the diversity of the customer communications requirements—operational, organizational, and functional—that must be supported. The resulting solution is a network of networks that must be melded to attain the required functionality, interoperability, and security across the Department in the near term. It also presents a long-term strategy by which the DON will build a more integrated and efficient Enterprise infrastructure over time. The “glue” that melds these networks together is the detailed description of network services, such as domain naming, directory, and security services, that provide the basis for network components to interconnect and operate.



The ITIA uses the basic construct of the Open System Interconnect model to address the transport and applications related layers that provide network connectivity and services. Figure 4.4-1 depicts the general layout of the technical framework. Throughout this array of network layers and entities, there is a well-developed and integrated description of network security mechanisms that form a “Defense in Depth.” The ITIA appendices provide specific guidance and decision-making tools (including performance metrics) for planners of metropolitan area and campus area networks.

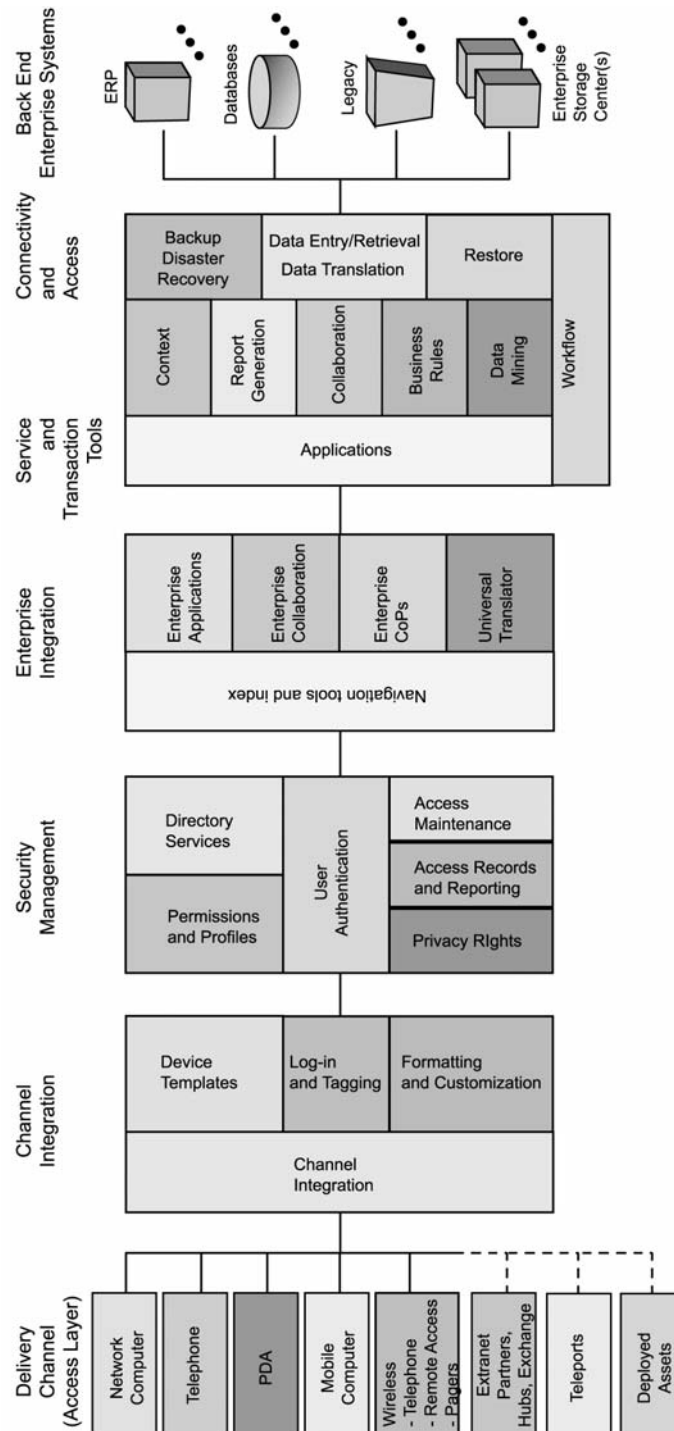


Figure 4.4-1—The ITIA uses the basic construct of the Open System Interconnect model to address the transport and applications related layers that provide network connectivity and services.

The ITSG amplifies the ITIA to describe how the components of the technical model must connect and interoperate at their boundaries. Again, since the Department was still focusing on how it should design and build multiple, decentralized network implementations that had to be complementary and interoperable, the ITIA allows planners, implementers, and acquisition personnel to anticipate changes in standards and specifications, thereby allowing multiple DON organizations that are implementing networks in a decentralized fashion to be successful.

IMPLEMENTATION

The ITIA development process was very similar to the development process described for the ITSG. Establishing the right membership on the team was critical, balancing organizational unit representation, and representation by true subject matter experts (regardless of organizational affiliation). Representation by people who could put their parochial interests aside and do what was best for the overall DON Enterprise was emphasized, and the team was kept small enough to be effective. Again, having the right people on the team was the key to success.



The ITIA will be updated to reflect the evolution of the DON infrastructure as a result of ongoing implementation of the Navy Marine Corps Intranet (NMCI). Under the NMCI contract, the greater majority of the computing and communications infrastructure is being provided as part of a performance-based services contract. The Electronic Data Systems (EDS)-led Information Strike Force will provide DON with the technical overlay of their commercial infrastructure and its interfaces to Information Technology for the 21st Century (IT-21), Marine Corps Tactical Data Network (MCTDN), etc. Once completed, the Department will integrate this effort into other planned product updates.

What Does Success Look Like?



Upon completion of the ITIA, the draft was vetted throughout the DON, and the final product was unanimously approved by the DON CIO Board of Representatives. This was a tremendously complex undertaking that required all of the Department's best and brightest IT technical personnel to make give-and-take decisions that could affect their planned decentralized network implementations. Having an IT Infrastructure Architecture in-hand and approved begged the question—how do we implement it? After much consideration from the senior levels in the acquisition community, with the ultimate decision made by the Secretary of the Navy, the ITIA became a critical foundation that facilitated implementation of a common, interoperable shore-based IT infrastructure through the NMCI initiative, and eventually to the NMCI contract.

4.5 Navy Marine Corps Intranet

NMCI provides the essential building blocks for security, interconnectivity and interoperability of the Navy and Marine Corps tactical and functional mission systems. NMCI represents an important strategic capability for the Navy and Marine Corps and is the most significant IT advancement in DoD.

—Tom Scruggs, Computing and Communications Infrastructure Team Leader

BACKGROUND

In the past, the Department of the Navy (DON) budgeted for and operated over one hundred different data and communications networks within the Department. Many of these networks featured their own locally developed, contracted for, and adhered to, standards and implementation schemes. This framework was fraught with inherent incompatibilities and functional duplications, restricting the adoption of modern network computing architectures that would have reduced/minimized costs. The Navy Marine Corps Intranet (NMCI) approach is a performance-based and cost-effective method to achieve a true Enterprise network based upon prevailing industry best practices. Following the requirements of the Clinger-Cohen Act of 1996, NMCI acquires information technology (IT) services at a fixed price, via a performance-based services contract that treats distributed IT services as a utility or basic platform for all Navy and Marine Corps business and communications. This approach is designed to meet specific performance requirements using incentivized Service Level Agreements (SLAs) that will measure network performance and end user customer satisfaction. The NMCI contract was awarded to an Electronic Data Systems (EDS)-led team known as Information Strike Force (ISF) on

The Navy and Marine Corps' new Intranet program is a model. Instead of just trying to buy, run, and maintain their own hardware and software, they outsourced the entire operation . . . That philosophy ought to be the rule, not the exception.

—Warren Rudman and Josh Weston, *Washington Post*, February 21, 2001

October 6, 2000.

APPROACH AND ORGANIZATION



NMCI is not an acquisition program in the traditional sense. Under the NMCI initiative, DON acquires commercial IT services through a performance-based services contract. The IT network, distributed platform, and associated support services are procured as a basic communications utility and paid for on a monthly basis. NMCI has been designated a Special Interest Initiative by the Office of Secretary of Defense (OSD), and DON and OSD have agreed that a tailored oversight framework is

appropriate.

The organization includes the traditional program office structure in DON as well as an oversight structure comprised of DON and OSD personnel. The Program Executive Officer for IT (PEO-IT), in his concurrent assignment as the Enterprise Acquisition Manager for Information Technology, is assigned responsibility for NMCI. For NMCI, the PEO-IT is supported by two program management offices, one for Navy and a separate one for Marine Corps. An Assistant Secretary of Defense Integrated Product Team has been given responsibility for oversight of the work that is in progress.



NMCI OVERVIEW

NMCI will become the Navy and Marine Corps' singular, common use infrastructure for the continental United States and selected overseas sites. NMCI will complement the Navy's shipboard Information Technology for the 21st Century (IT-21) and the Marine Corps Tactical Data Network (MCTDN), providing a worldwide reach-back capability for Navy and Marine Corps deployed forces (see Figure 4.5-1).

The NMCI service contract encompasses everything necessary to ensure the transmission of data, voice, and video information. It includes capital infrastructure improvements and the accompanying maintenance, training, and operation of the NMCI infrastructure. In an effort to ensure that the Department made the most of the capital investments it had been making in IT, DON put an exchange-sales clause in the contract where the vendor would make an equitable cash adjustment to their proposed seat costs and the DON IT infrastructures would be turned over to the vendor. The service provider will own and maintain all required desktop and network hardware and software, and provide all required IT services, including pier connectivity. The NMCI solution includes 17 seat types.

One of the key accelerant factors to ensure that NMCI does not become technologically obsolete in today's ever changing technology environment is that the Contract Line Item Numbers (CLINs) are regularly updated so that the product that ships is at the 75 percent level of the state-of-the-art on commercial shelf at the time of shipping.

One of the first reactions when people look at the CLIN prices is that they feel they can get a better deal by walking into any computer store. That reaction is quickly turned around once people realize that NMCI's seat costs include all the services shown in Figure 4.5-2.

Perhaps most critical to the entire NMCI concept are the 44 Service Level Agreements (SLAs). These SLAs are tailored to support the unique mission requirements of Navy and Marine Corps users. For example, seat types include those for embarkable users, remote users, and thin client users. Services include support of all DoD applications. The SLAs provide over 633 separate metrics to ensure that delivered services meet the expectations of NMCI customers.

The available end user software includes a "Gold Disk" of standard office automation tools that are included on every desktop. Users will be able to have additional applications pushed to them from the Network Operations Center (NOC). The NMCI architecture

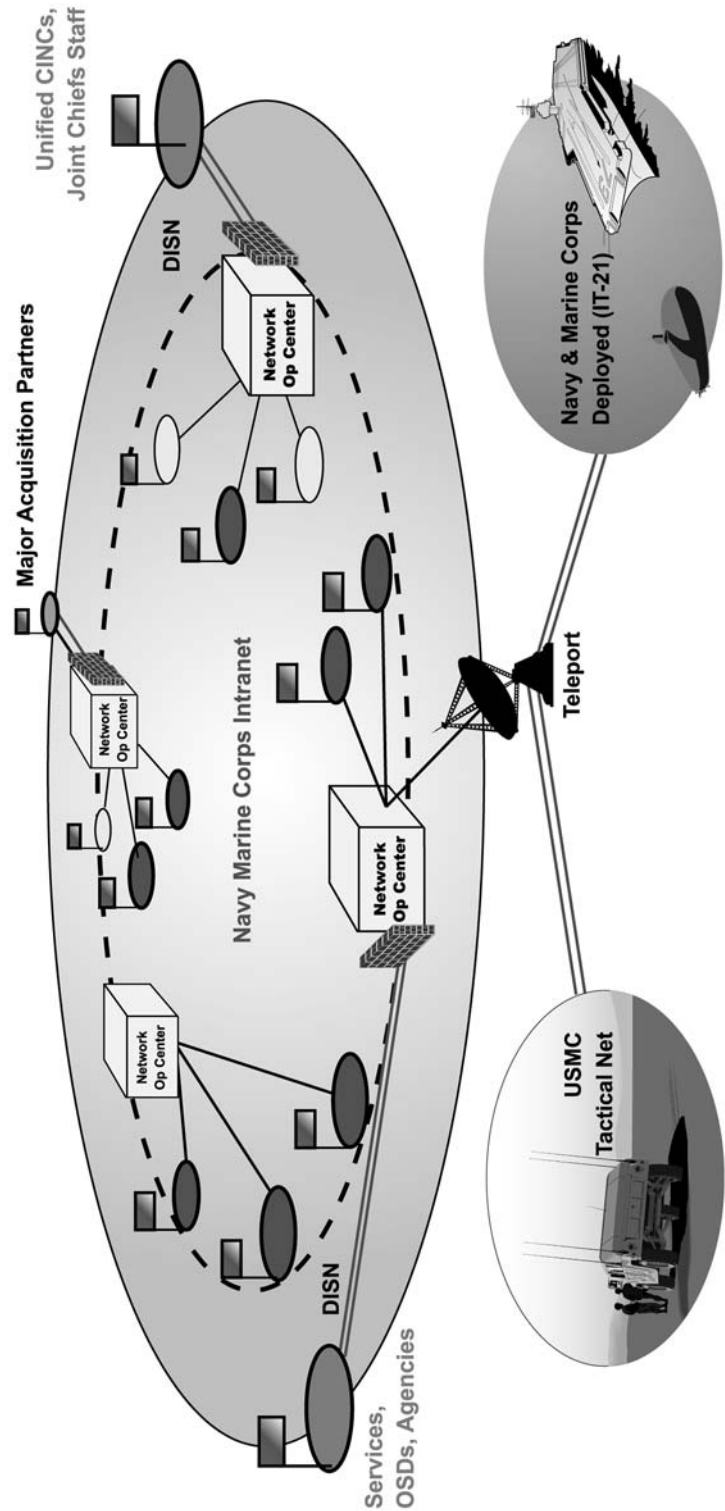


Figure 4.5-1—DON Enterprise Architecture World Class Design

includes six NOCs, two Enterprise help desks, and 72 server farms. All users receive their support from this consolidated, centralized management structure. Elements of NMCI are interconnected via a high performance WAN that ensures continued support over the life of the NMCI contract through the concept of bandwidth on demand. Information assurance for NMCI is unusually robust because of a layered system of defenses that provide protection from intrusion, service denial, and compromise. Access to the information exchange partners outside NMCI is controlled via one of the six NOCs to ensure integrity of system defense. NMCI will be installed in multiple increments to occur over two years. The first increment supports 60,000 users and includes a test and evaluation and proof of concept reviewed by OSD and Congress before continuing with the remainder of the installation. At full implementation NMCI will include approximately 411,000 seats. In order to receive full payment for the seats, the ISF is required to demonstrate and meet the seat performance SLAs. The contractor will also be awarded incentive payments or assessed penalties, depending on their performance in selected areas as listed in Figure 4.5-2.

Besides meeting the SLAs for payment, the ISF is also monitored and can obtain additional incentive payments for small business performance, security, and user

<ul style="list-style-type: none"> ▪ Security Services (firewalls, intrusion detection, encryption) ▪ CAC/PKI Implementation ▪ Wide Area Network Access (DISN, Commercial WAN, Internet) ▪ Infrastructure (voice, video & data transport) ▪ Joint and Industry Network Interoperability ▪ Pier Services (connectivity, NOC/JFTOC interface) ▪ Enterprise Functions (Help Desk/Tech Support) ▪ Network Mgmt. Services 	<ul style="list-style-type: none"> ▪ Desktop Hardware (standard, high-end, and laptop) ▪ Desktop Software (standard software suite) ▪ Organizational Messaging (AUTODIN, DMS) ▪ Training ▪ Directory Services ▪ E-mail ▪ Remote Telephone Access ▪ Domain Name Service ▪ Help Desk/Tech Support ▪ LAN (building LANs) ▪ System Mgmt. Services
--	--

Figure 4.5-2—The NMCI contractor will be awarded incentive payments or assessed penalties depending on their performance in these NMCI service areas.

satisfaction. Over 50 percent of the incentive pool is reserved for customer satisfaction.

SECURITY

The basic Information Assurance (IA) strategy requires implementation of a Defense in Depth approach that provides basic security services for all information being transported over the NMCI: confidentiality, integrity, availability, authenticity, identification, access control, and non-repudiation. Although the use of commercial best practices is encouraged, NMCI also meets all mandatory security requirements, such as use of the DoD Public Key Infrastructure (PKI), DoD Common Access Card requirements, and certification and

accreditation in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

Although the NMCI contractor is responsible for the design, implementation, and operation of NMCI, authorized DON personnel will perform a number of critical security roles. These roles fall into two categories: (1) ensuring that the security of the NMCI satisfies Federal, DoD, and DON requirements, and (2) exercising essential command authority over DON Defensive Information Operations.

INTEROPERABILITY

The NMCI contract provides detailed guidance to ensure that NMCI meets DoD Global Information Grid architecture requirements, and can satisfactorily interface with all DoD and Joint networks and applications.

The NMCI provides aggressive interoperability testing both at initial test and evaluation (T&E) and during subsequent NMCI operation. The interoperability requirements contained within the SLAs can be viewed as the equivalent of information exchange requirements (IERs). In this parallel, there is a defined effort to determine, in required detail, that interoperability requirements are sufficiently defined and that support is applied to ensure these requirements are met. This will be reflected in the NMCI Interoperability Test Plan (ITP). This ITP represents a new approach to interoperability management; no similar initiative is in place, so innovation will be required and the use of commercial off-the-shelf (COTS) tools emphasized. The contract strategy was to specifically ask the contractor to develop this model using commercial best practices, COTS tools, contractor processes, and other appropriate sources.

The NMCI interoperability model will use an integrated set of sensors to detect negative occurrences. These sensors require granularity of measured performance and encompass more than access to applications. For all relevant performance areas (expressed in the 23 interoperability metrics defined within the SLAs), the focus is foremost on those services that DON stakeholders need to perform their missions. The ITP will establish thresholds for each reporting area and set requirements for notification and intervention. For the end user, the sensors will reflect the ability to access legacy applications—both Joint and DON.

Test and evaluation is a significant event in the first increment targeted at the Naval aviation community. The results of T&E will be one of the primary inputs to the assessment of NMCI during the strategic pause by OSD and Congress for determining whether NMCI should proceed to full implementation. Four sites are selected for T&E. A Baseline System Assessment (BSA) will be conducted at these four sites to characterize the existing environment. The BSA will be followed by a three phase contractor T&E, and then an Operational Evaluation (OPEVAL).

The overarching operational requirement against which NMCI will be tested is to ensure that the change from legacy networks to NMCI allows Navy and Marine Corps commands to continue to accomplish their missions and that the expected performance

enhancements—in areas such as security, interoperability, reliability, and network operations and maintenance—are achieved.

BEST PRACTICES

NMCI differs from typical IT acquisition programs because it expressly does not specify solution elements of the service such as bandwidth or the desktop solution and software. This NMCI strategy provides a distinct advantage to the government. The Contractor must collect data, assess communications requirements, and then provision enough bandwidth to meet a comprehensive set of defined, measurable service levels. There is further advantage to the government in that the ISF must maintain that level of service over the life of the contract at no additional cost. In other words, as the DON user requirement grows, the ISF is required to increase bandwidth to maintain the stated level of measured service.

To adequately define the expected level of delivered service, the 44 SLAs (each with from 3 to 12 separate metrics, and each of those with three levels of service) specify over 600 separate metrics. For networking, SLA metrics include availability, latency, packet loss, loading factor, interoperability, and time to restore service. For end user service, metrics include desktop hardware performance, e-mail and other server-based services, and help desk effectiveness. For security, examples include metrics such as denial of service and accuracy of PKI certificates.

The NMCI fully embraces and implements the best practice principles of the Clinger-Cohen Act (CCA).

- Using industry best practices, NMCI will improve DON's ability to focus on its warfighting and support missions. NMCI makes use of commercial services by adopting the same seat management approach to IT sourcing used in commercial industry.
- The NMCI test and evaluation in the first increment complies with CCA's provision for IT pilot programs.
- As part of the NMCI effort, the DON will be fully compliant with the Joint Technical Architecture (JTA), Naval standards and architecture plans, and the emerging DoD Global Information Grid (GIG).
- The DON is taking an accepted industry cost assessment approach using the Gartner Total Cost of Ownership Model across the Department that will quantify the net cost and performance benefits of NMCI.

BUSINESS CASE ANALYSIS

The Office of Management and Budget (OMB) has required the DON to assess the results of the NMCI first increment deployment against cost, schedule, and performance goals established for the acquisition as specified in the NMCI contract. The DON has developed a Business Case Analysis (BCA)-based approach that compares the pre-NMCI IT direct costs and performance levels (baseline) to the direct costs and performance levels of NMCI measured in the first increment. Pre-NMCI costs will be based on cost data from the original BCA and from additional site surveys that are being conducted at select first

increment sites. These pre-NMCI baseline costs will be compared to the actual costs and performance of NMCI during the first increment. In order to establish the baseline of pre-NMCI IT performance, the Commander, Operational Test & Evaluation Force (COTF) and ISF will perform a complete Baseline Systems Assessment (BSA) of the first increment consisting of data collected through end-user surveys, IT/CIO interviews, and collection of available technical data. This performance baseline is then compared to NMCI performance data including the SLAs.

It should be noted that because of the NMCI solicitation effort, the DON had to select traditional technical support contracts for non NMCI work only when the vendor had signed statements that they would not play in the NMCI space. When the original BCA was presented to Capitol Hill, DON was asked to provide an additional independent assessment of the BCA. The DON went outside of the traditional government contractor spaces and focused on the Big 5/6 accounting firms, or their IT arms, to conduct this review.

BUDGET

It is estimated that in recent years the DON has spent \$1.6 billion annually on basic distributed computing information services and connectivity for personnel in the continental United States. IT hardware, software, and support has traditionally been managed by region, or locally at the organizational level, with no standardized procurement or installation process or Enterprise-wide system standards. The budgetary resources to support NMCI are managed on a distributed basis throughout the Department, with decentralized requirements generation and budget formulation, and centralized contract execution by the Navy's Space and Naval Warfare Systems Command (SPAWAR) and the Marine Corps Systems Command (MARCORSYSCOM) based on claimant reimbursable funding. This contract allows the DON to achieve significant economies of scale by purchasing IT services from a single entity, thus capitalizing on an Enterprise aggregation of service requirements, and adopting a consolidated regional/Enterprise management of the service execution and operation. Estimated costs (for equivalent or better services) under the NMCI contract are \$1.2 billion annually, and represent significant potential cost-avoidance to the government.



PERSONNEL

The NMCI strategy includes mitigation for any adverse implementation impacts of NMCI on the DON Military and Civilian IT workforce. While DON activities did not previously possess many end-to-end capabilities provided by NMCI, DON did operate and administer IT networks and provide communication services at the local level using Civilian personnel support. Consequently, when DON transitions to NMCI, some network administration, operations, and communications positions will be displaced. The DON is making a concerted effort to retain affected IT workers by transferring them into other important IT areas within the Department, such as legacy systems support and applications development. In addition, for Government Civilian workers who wish to continue in network and communications related jobs, the ISF is required to offer comparable positions to qualified employees for employment openings under the contract.

The ISF has contractually committed to hire qualifying employees who desire to transition, at an increase in salary and with a guaranteed period of employment.



CONCEPT PUT TO THE TEST

Upon return to the Pentagon after the tragic events of 9/11 and surveying the initial damages, the Department of the Navy realized it was faced with the immediate restoration and reconstruction of much of its communications capabilities that had previously existed in the Pentagon. The initial damage estimates ranged from total reconstruction of the Navy Command Center (NCC) and Navy Budget Office, which were totally destroyed, to the rebuilding of its classified and unclassified networks in temporary office spaces.

Using the NMCI contract as the prime vehicle to undertake this effort, EDS was called on Wednesday (9/12) and told to set up a temporary NCC

capability in the Marine Corps Command Center. This center was operational by midnight on Friday and would be moved and reconstructed back inside the Pentagon once space was re-allocated.

Temporary spaces were allocated between the Washington Navy Yard, Navy Annex, and National Center Two (NC2) in Crystal City. On Wednesday evening (9/12) EDS was given a preliminary estimate of the number of NMCI seats the Department would need to reconstruct its lost capabilities, and EDS and the ISF went to work. A call was put out for all available cablers, network engineers, and setup specialists from up and down the mid-Atlantic region to descend on Washington, DC.

Thursday morning (9/13), nine 18 wheelers left EDS's staging facility in St. Louis, MO filled with 860 portables, 335 desk side computers, and enough CAT-5 cabling and fiber optic backbone cables to outfit five floors of office space. A separate 18 wheeler left Cisco headquarters in San Jose, CA with all of the routers and switches necessary for completion of the outfitting. Separately on Thursday, the Department of the Navy secured five floors of space in NC2 and set up additional space in the Washington Navy Yard in order to rebuild the Navy Budget Office, which lost its 30 servers in the attack.

Friday morning (9/14), all the equipment that had left St. Louis, MO on Thursday arrived at the Navy's NMCI warehousing facility in Naval Air Facility Washington, and tear down began. The equipment was separated into pallet loads corresponding to the floor density in NC2. The EDS ISF Team knew that they had their work cut out over the weekend to load software on approximately 1,000 machines following delivery to Crystal City in Arlington, VA.



Over the weekend, the EDS ISF Team was allowed to move into the NC2 spaces and the Washington Navy Yard to begin work to create a network and server farm where none had existed. By Sunday (9/16), 50 PCs were operational in the Washington Navy Yard as well as the new server farm for FMB, the Navy's Budget Office.

Crisis relocation and reconstruction efforts were completed on Wednesday (9/19). Using the NMCI vehicle as the single point of implementation allowed DON to rapidly recreate all of the capabilities lost in the attack on the Pentagon. NMCI allowed the Department to bring roughly 700 people back online within a week of the attack.

CONCLUDING THOUGHTS

NMCI provides comprehensive, end-to-end information services to the Navy and Marine Corps through a common computing and communications environment. It will provide DON access, interoperability, and security for information and communications through Enterprise data, voice, and video services for all Navy and Marine Corps personnel. NMCI will complement IT-21 and MCTDN, providing a worldwide reach-back capability for Navy and Marine Corps deployed forces. The NMCI contract is on a fixed-price basis, to deliver to the government robust, interoperable, and secure information exchange services for all NMCI operational and functional users.

4.6 IT Enterprise Architecture

The development, implementation, and maintenance of an Enterprise Architecture facilitates improved interoperability, application integration, and business processes. It provides the foundation for developing measures of effectiveness and systems engineering.

—Brian Wilczynski, DON CIO Architecture Team Leader

BACKGROUND

The Clinger-Cohen Act assigns agency CIOs responsibility for developing, implementing, and maintaining an information technology (IT) architecture. The architecture provides the capability for organizations to align IT investments with organizational missions and strategies. It also provides the means for developing migration and integration strategies for current and planned systems. The office of the Department of the Navy Chief Information Officer (DON CIO) has discovered that several key elements contribute to the success of an agency-wide architecture development and management effort. The following key elements are discussed in detail in this section:

- Architecture framework
- Articulation of benefits
- Senior-level commitment
- Architecture policy
- Tools, repositories, and training
- Architecture integration

THE ARCHITECTURE FRAMEWORK

An Enterprise Architecture (EA) is the documentation of current and desired relationships between business process/warfighting activities and the supporting information technology. OMB has specified that the EA include the following components:

- Business processes
- Information flows and relationships
- Applications
- Data descriptions and relationships
- Technology infrastructure
- Technical reference model and standards profile

It is not only essential to explicitly capture these components; it is essential that they are collected in a consistent format that promotes integration. For example, if the personnel community within an Enterprise documents its business processes, information flows, and data descriptions, they should be consistent where they overlap the financial community within the Enterprise. This is accomplished through the use of a framework for architecture development.

The architecture framework for an agency should provide the rules and specifications for developing and presenting architecture descriptions that ensure a common denominator for understanding, comparing, and integrating architectures. Within the DoD this is facilitated through the DoD Architecture Framework. The DoD Framework recognizes three different views within the overall EA (see Figure 4.6-1). These views and their content are:

- **Operational:** A description of the tasks and activities, operational nodes or elements, and information exchange requirements between nodes. Nodes can be organization types or actual organizational entities.
- **Systems:** A description of the systems and interconnections used to satisfy operational needs and the platforms and facilities with which they are associated. Interconnections include the supporting network infrastructure as well as the interfaces between systems.
- **Technical:** The set of rules governing the arrangement, interaction, and interdependence of system parts or elements.

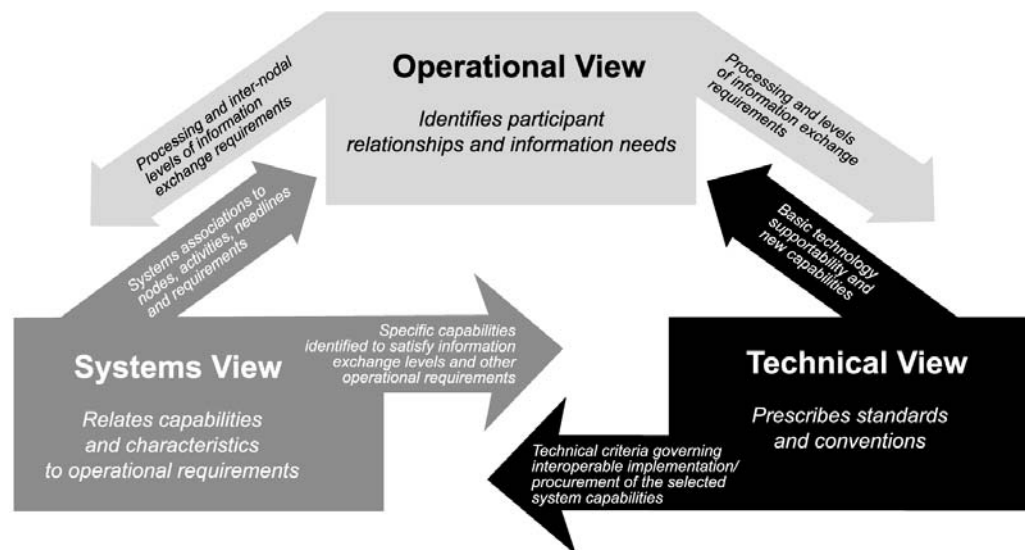


Figure 4.6-1—The three views within the Enterprise Architecture Framework include:

Operational = business processes + information flows and relationships

Systems = applications + data descriptions + technology infrastructure

Technical = technical reference model and standards

For each of these views within the Framework, specific products are identified that are to be constructed. These products are both textual and graphical. The Framework not only identifies the products that describe each view, it describes each product in terms of the data required to build them. The use of a standardized data structure for building the products allows them to be stored in an architecture repository that provides the ability to conduct analysis and integration of the architectures. Repositories will be discussed in more detail in the “Tools, Repositories, and Training” section.

An architecture framework describes how and what architecture products are developed. The framework does not, however, specify how the products will be used. Without a clear objective of what benefits are to be derived, an EA effort will lack focus and collapse upon its own weight.

ARTICULATION OF BENEFITS

Many Federal agencies have engaged in monumental efforts to document their business processes in support of reengineering. Many of these costly efforts have failed to produce measurable results. Success of the EA will depend upon clear articulation of the following:

- Intended use of the architecture
- Scoping of the architecture effort
- Required characteristics to be collected
- Architecture products that will be produced

Plans for how the architecture products will be used should be specified before the effort begins. The EA is an essential supporting element of the capital planning process, interoperability assessments and improvements, security strategy, data integration efforts, and systems migration strategies. While a comprehensive and integrated EA will support all of these areas, the timeline for its development may be prohibitive. Priorities that will be accommodated as the architecture evolves over time need to be established. For example, while an agency may identify interoperability as a major problem area to be addressed by the architecture, there may first be a need to conduct focused systems migration efforts to reduce the sheer numbers and complexity of systems and databases. In this case, the articulation of this intended use of the architecture will impact the products that are developed and their level of detail. Once the migration efforts are completed, the architecture can evolve to the level of detail required to address interoperability problems, many of which may be eliminated through the migration effort itself.

SENIOR LEVEL COMMITMENT



Development of an EA is a lengthy and expensive effort. Without buy-in from senior leadership, the EA will not receive the funding nor the human resources required to support its development. Buy-in is essential not only within the IT community, but across all organizations within the Enterprise. The benefits of the EA must be clearly defined and communicated to senior leadership. Where possible, best practices and case studies should be cited. Development of a business case that outlines the cost of developing the architecture and a projection of the savings to be achieved are also highly recommended. The business case should identify both direct and indirect benefits to be achieved.

The continued engagement of senior leadership is essential. For this reason, an Executive Architecture Steering Committee should be established. Those organizations held accountable for the architecture's development and implementation should be required to report progress to this committee periodically. The committee must take an active role in providing direction and policy.

ARCHITECTURE POLICY

Without clearly defining the requirement to develop the EA, and the assignment of roles and responsibilities within the agency, the effort would be fragmented. Accountability within the organization must be established to ensure results with clearly defined measures of performance stated for those individuals and organizations held accountable for the development and management of the EA.

The role of the CIO is to develop policy and define the framework and processes for creation of the EA. It is unrealistic, in most Federal agencies and industry organizations, to expect that the CIO will be able to execute development of the EA without the contributions of the business units and systems' owners. The policy, therefore, must follow a centralized planning/decentralized execution model. In addition to the CIO role, other stakeholders to consider in the policy include financial managers, process owners, and acquisition program managers. Without inputs from each of these entities, the EA will be incomplete. In the context of the DoD Architecture Framework, the process owners/warfighters are responsible for the Operational view, acquisition program managers are responsible for documenting the Systems view, and the CIO is responsible for defining the Technical view. The role of the financial managers is two-fold: identification of funding to support the EA development and oversight. In their oversight role, financial managers must incentivize development and use of the architecture.

TOOLS, REPOSITORIES, AND TRAINING

A standard suite of tools to be used in developing architecture products needs to be defined to ensure consistency across the Enterprise. Few tools exist that can support all of the many formats of architecture products (textual, graphical, tabular). The tool suite will generally consist of a combination of commercial off-the-shelf (COTS) word processing, graphics, and spreadsheet applications, databases, and some specialized Computer Aided Software Engineering (CASE) tools such as those for activity and data modeling. In addition to the applications required to capture the necessary architecture products, analytical tools such as spreadsheet add-ons, activity-based costing programs, and simulation applications need to be considered.

An important component of the tool environment is the architecture repository. Development and support of this component will generally be the most expensive and should be planned very carefully. In addition to providing a centralized library of architecture products (or artifacts, as they are commonly referred to), an architecture repository provides the ability to conduct analysis and integration of related architectures developed independently. It is essential to establish a configuration management plan for the repository, including the means by which to standardize terminology across the Enterprise. Standard terms for processes, organization types, information exchanges, data elements, and applications are essential. Without this type of management, comparing and integrating architectures cannot be done, resulting instead in efforts that are "stovepiped" and fail to satisfy the rigorous requirements of a true EA.

Within the Department of the Navy, the Chief Information Officer has sponsored development of a DON Integrated Architecture Database (DIAD) for the capture of architecture data. The DIAD is based upon a DoD standard data model known as the Core Architecture Data Model (CADM). The CADM includes all of the data requirements needed to support the products specified in the DoD Architecture Framework. The DIAD was developed in Microsoft Access and is distributed on CD, providing portability, and is inexpensive for DON commands to install and use. Data collected in the DIAD can be integrated in a master database where terminology can be standardized. Because of its CADM “genealogy-genealogy,” the DIAD can exchange data seamlessly with other architecture repositories that are also CADM-based, including the DoD’s architecture repository currently under development. The DoD repository will provide the ability to develop an integrated Joint architecture for the Defense Services and Agencies. The DIAD has been selected by DoD as the model for its current architecture development efforts.

To effectively use the selected tool suite and repository, users require adequate training. The training program should be established prior to initiation of architecture development efforts. Training should not be limited to use of the tools, but also include a detailed review of the architecture framework, its products and their relationships, and intended usage of the architecture in support of capital planning, interoperability assessment, and systems migration.

With senior-level commitment and buy-in to the effort and its benefits, an inclusive policy to engage the Enterprise, and the tools and training needed to support architecture development, the architecture will evolve. As it is developed in a decentralized manner, it will become necessary to integrate the architecture products into an Enterprise-level representation.

ARCHITECTURE INTEGRATION



An architecture integration strategy is developed in advance of developing any of the products. The true value of an Enterprise Architecture cannot be realized without the ability to integrate independent efforts. The policy covers roles and responsibilities related to integration, which needs to be conducted at a high level in the Enterprise. A prerequisite to integration is the use of a repository that captures architecture data in a standard format. The CIO is the EA integrator. Integration is no small effort, and a core team established within the CIO organizational structure helps support it.

In addition to a chief architect responsible for overall program oversight and leadership, a lead architect for each of the major architecture components is designated to include: business architect (processes), information architect (information flows and relationships), applications architect (systems/applications), security architect (security strategy and standards), infrastructure architect (communications and computing infrastructure), and standards manager (maintains the Enterprise IT standards required for interoperability). In addition to the standards manager, the CIO designates the appropriate individuals/organizations to represent the agency in Federal, Department, commercial, and international standards bodies.



DON CIO ARCHITECTURE AND INTEROPERABILITY

Within the office of the DON CIO a team has been established to provide the leadership, policy, framework, tools, and coordination of architecture development. The government staff is relatively small in comparison to the support component of the team. This support component consists of both industry personnel with expertise in architecture development and subject-matter experts from across the DON. The subject-matter experts participate in DON CIO-funded Integrated Product Teams (IPTs) that meet to develop the architecture products and corporate processes required to support EA integration. Through the use of this IPT approach, the DON CIO developed the Information Technology Standards Guidance (ITSG) and Information Technology Infrastructure Architecture (ITIA), two main components of the EA, over a two-year period. Current efforts are focusing on implementation of a program to develop the Operational and Systems views of the DoD Framework. The DIAD will support the capture and integration of architectures developed across the myriad of functional areas within the DON. This effort is closely aligned with data management efforts, which are focused on the identification and migration to authoritative data sources, the integration of data, and consolidation of databases. Data Management is discussed in the next section.



4.7 Data Management

The most difficult task for the CIO is the development of an Enterprise-level data architecture. The benefits to the Department in improved interoperability, security, data quality, and more efficient data storage and distribution, however, far outweigh the difficulties.

—Brian Wilczynski, Data Management Team Leader

BACKGROUND

Data is a core Enterprise asset; applications are developed and procured to support the generation, manipulation, and exchange of data required to execute agency missions. The Clinger-Cohen Act requires agencies to demonstrate that IT investments directly support core mission functions. To do this effectively, the Enterprise must understand its data requirements and existing assets. This requires that the DON CIO, as the senior IT leader for the agency, take an active role in developing a data management strategy for the Enterprise. A key element of the data management strategy is development of the data architecture (the data descriptions and relationship component of the Enterprise Architecture).

Data management has many facets: data quality, data standards, data storage, and security. The most difficult task for the CIO is development of an Enterprise-level data architecture that minimizes redundancy, promotes interoperability, and ensures integrity of the data used across the Enterprise. An Enterprise data architecture not only improves security and interoperability, but increases data quality and provides efficiency in data storage. In November 2000, the Office of the DON CIO completed a year-long effort focused on defining the policy, processes, and tool requirements to support development of the data architecture. This effort is called Data Management and Interoperability (DMI).



Since data is exchanged across organizational and functional boundaries, development of a data architecture requires representation of the major functional domains within the Enterprise (personnel, finance, logistics, intelligence, procurement, combat systems, etc.). The DMI effort was conducted through an Integrated Product Team (IPT) of data management experts from over 40 Navy and Marine Corps commands. The DMI IPT addressed three major areas:

- Data Management Policy: Policy, roles and responsibilities, budgeting, and requirements.
- Architecture and Standards: Processes needed to support the development of functional and Enterprise data architectures.
- Repositories and Tools: Requirements for an Enterprise meta-data repository and data modeling and engineering tools.

Each of these three areas is key to establishment of an Enterprise data management program. This section addresses the requirements for developing a data architecture that supports Enterprise data quality, integrity, security, and interoperability objectives. The

management of data at a corporate level will facilitate database consolidation, and data integration, and result in the identification of authoritative sources of data.

DATA MANAGEMENT POLICY

Most data-related problems within the Enterprise are not so much technical challenges as they are management issues. The inability to share data seamlessly across organizations and functional domains is largely a result of stovepiped development of applications and databases to support specific activities. A management structure capable of addressing cross-organization/cross-function typically does not exist in large Federal agencies. Within the DON, Functional Data Managers (FDMs) are being identified in accordance with policy. These FDMs will have responsibility for facilitating documentation of existing data assets, defining functional data requirements, and participating in development of the Enterprise data architecture

Data management policy should support a set of guiding principles that are supported by senior leaders. For example, a guiding principle may dictate that “Data will be entered once and reused many times across the Enterprise” or that “Databases will be consolidated through the integration of data from disparate sources into Enterprise authoritative data sources.” In addition to establishing guidelines for how data will be managed, the policy defines roles and responsibilities. The CIO has responsibility for defining standardized processes, techniques, and tools to support an Enterprise data management program. FDMs execute development of the data architecture as defined by the CIO. In addition to FDMs and the CIO, systems developers are key participants in the data management process; their collaboration will result in development of the best data architecture and standards for the Enterprise.

ARCHITECTURE AND STANDARDS

Just as there is a need for an architecture framework for the Enterprise Architecture, the products and processes associated with the data architecture must be defined. Under a centralized planning/decentralized execution model, both functional and Enterprise data architectures are developed. Products include: existing physical database structures, logical models of data requirements, and mappings of the physical data structures to the logical models.

Logical data models are used to describe the Enterprise data requirements at a high level. Logical models need to be developed at the Enterprise and functional domain levels and are developed using subject matter experts from the major functional domains of the Enterprise. Physical data structures are captured from existing systems by database administrators and developers and are mapped to the logical models by FDMs. These mappings provide the capability to eliminate redundant data elements and assist in identifying data requirements that are not being met by existing databases. The key enabler of logical and physical modeling is an Enterprise meta-data repository.

REPOSITORIES AND TOOLS

Meta-data is the language of data management practitioners. Literally “data about data,” meta-data describes the characteristics of data used by the Enterprise. Typical meta-data includes: data element definitions, data types, character length, units of measure, and domain values (lists of accepted values). The standardization of meta-data across the Enterprise facilitates the seamless exchange of data between automated systems. The development of a data architecture and standards requires visibility of data assets (logical and physical) to systems developers and domain subject matter experts. This visibility is provided through an Enterprise meta-data repository.

The meta-data repository is a library of data models and data descriptions. Systems developers register physical data structures, and the systems in which they reside, in the repository. This registration process is then incorporated into acquisition guidelines. Documentation in the repository is specified as a deliverable in the Contract Data Requirements Lists (CDRL) for every systems development effort.



The DON CIO has sponsored development of an Enterprise meta-data repository called the DMI Repository (DMIR). Members of the DMI IPT established the requirements and specification for the DMIR. The DMIR is a Web-accessible database that is based upon the DoD Core Architecture Data Model (CADM). As noted in Section 4.6 “IT Enterprise Architecture,” the CADM is the foundation for the DON Integrated Architecture Database (DIAD) that the DON CIO has developed to support development of the Enterprise Architecture. The use of the CADM standard in both databases allows the seamless exchange of data that is common between the two repositories. This common data includes system names and point-of-contact information for the systems.

The data architecture is a component of the overarching Enterprise Architecture (EA). As with the overarching EA, the data architecture requires senior-level commitment, policy, and supporting tools. A detailed discussion of the requirements for DMI within the Department of the Navy is available in the DMI Implementation Planning Guide located on the DON IM/IT Web site at www.don-imit.navy.mil. This Planning Guide is the capstone document of the DMI IPT.

4.8 Electromagnetic Spectrum

The electromagnetic spectrum is a finite and natural resource which is absolutely critical to our National security. The effective management of spectrum requires a curious and parsimonious mix of physics, politics, economics and diplomacy.

—John J. Lussier, Spectrum Team Leader

BACKGROUND

The ability of Naval Forces to support diverse operations and crises is largely dependent on their ability to communicate. Uniquely, the Navy's SEAL Teams, submarines, and Battle Groups, along with various Marine Corps units deployed aboard Amphibious Ready Groups, are often first to arrive in a theater and must rely on the wireless electromagnetic spectrum to remain highly maneuverable, flexible, and tactically effective. In the last few years, the rapid adoption of commercial communication technologies has taxed spectrum resources. Domestic and international companies, and even civil agencies, are putting pressure on their governments to allocate more spectrum to commercial applications. In the United States, much of the spectrum under discussion is dedicated to U.S. Military missions. Worldwide, many governments interested in promoting their telecommunication services consider this reallocation of spectrum simply as a way to generate revenue. Most are not fully aware of the impact on Joint Military operations and international security. As the Civilian sector moves forward with faster, more convenient, and less expensive communication platforms, the Military Services are under increasing pressure to vacate more spectrum and modify operational Military systems.

The notions of warfare are undergoing radical change. Industrial Age warfare, historically based on massive forces and attrition, is rapidly giving way to the understanding that forces best able to effectively employ information technologies have the advantage. The Department of the Navy (DON) forces must achieve and maintain a level of information superiority never before attained. They must have the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. To meet this challenge, the DON has developed the Network Centric Warfare concept, outlining the way it will organize and fight in the Information Age. As an information superiority-enabled concept of operations, Network Centric Warfare increases combat power by networking together sensors, weapon systems, decision-makers, and warfighters. The advantage is enhanced and shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a high degree of self-synchronization. The electromagnetic spectrum is the key enabler of Network Centric Warfare.

Increasingly, "speed of command" will decide engagements where the precise placement and timing of both forces and effects are substituted for traditional notions of combat mass. In such an information rich and highly mobile environment, spectrum emerges as the lifeblood of the battlefield.

As a Department, acting in the best interests of the American people, the DON must conscientiously apportion this limited resource between spectrum wants and actual warfighting spectrum needs. In order to accomplish this, the DON must demonstrate the efficient use of current spectrum assignments as well as effectively engage new technologies that will improve the use of the spectrum or reduce the amount of spectrum required.

The overriding objective to develop a proactive, time phased spectrum management strategy based on Naval warfare requirements will allow the DON to make spectrum transparent to its warfighters. Then our forces will be able to operate any time, any place with superior capabilities.

DESCRIPTION OF INITIATIVES

The Department of Navy Strategic Vision for Spectrum was developed to identify and proactively manage spectrum issues crucial to DON operational capabilities and outline leadership roles within the Navy and Marine Corps. The Department of the Navy Chief Information Officer (DON CIO), the Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN (RD&A)), and the Navy and Marine Corps Chief Information Officers together will evaluate current and future operational and acquisition requirements. The goal of the Strategic Vision is to create the foundation for development of an innovative, entrepreneurial, long-term spectrum management strategy based on evolving Naval warfare requirements. This goal encourages the DON to support development of the overall Department of Defense (DoD) spectrum strategy, foster sharing and compatibility with commercial entities, recognize creative approaches to warfighting requirements, and establish professional relationships with industry groups, research laboratories, academics, and the operational DON components.

The Strategic Vision was developed in light of the changes in the way warfare is conducted, the tremendous increase in the demand for spectrum access throughout the world, and emerging threats from terrorism. Assured spectrum access is vital to maintaining our national security and Military superiority and our responsiveness to events that challenge our interests at home and abroad.

The Navy has a unique challenge among the Military Services, because Navy command and control centers are afloat assets with no direct access to commercial or Military communications systems via landline. The only access to these vital communication resources by commanders at sea is via wireless links. A broad range of the spectrum may be required to support the functions of even a small collection of these communication networks. Spectrum allocation management becomes more complex as the number of systems using it increases.

Our command, control, communications, computer, intelligence, surveillance and reconnaissance capabilities are structured to provide Naval Forces with a seamless transfer of information that allows freedom of action and limits vulnerability during both combat and non-combat operations. The capabilities of the Department of the Navy's significant inventory of radio frequency (RF) spectrum-dependent systems can be loosely categorized as those that communicate information in the form of audio, video, or digital data; and weapon systems sensors such as radar, electronic warfare systems, and navigation systems.

Strategic Vision is not confined to the notion that DON policy and management is focused solely on radio frequency systems. The DON is dependent on spectrum above radio frequencies for line of sight data transmission, weapon systems target acquisition and designation, countermeasures devices, advanced satellite imagery, and analysis of energy sources from space based platforms.

Technologically superior and precise equipment has been critical to our combat successes. Even the simple act of dropping a bomb has spectrum allocation implications. The Joint Direct Attack Munition (JDAM) program upgrades general purpose and penetrator bombs. Installed as a tail kit, it provides each weapon with an all-weather, autonomous, high accuracy, conventional bombing capability. On-target delivery of a JDAM can involve 30 events of spectrum consumption. DON must strive to maintain its technical warfighting advantage as it faces a wider and asymmetrical range of threats from savvy adversaries.

The DON's spectrum-dependent systems are selectively integrated aboard Navy/Marine Corp platforms and within Military units to provide the capabilities needed to accomplish various assigned missions. For example, a Navy aircraft typically hosts many spectrum-related devices. First, voice communications and digital data links are supported by one or more radios. Next, guidance and navigation systems include a radar altimeter, tactical air navigation, Global Positioning Systems (GPS), and an instrument landing system. Also, weapon systems, with associated fire control radar, may include radio- or laser-guided bombs and missiles. Finally, sophisticated electronic warfare systems exist to detect and suppress enemy radar and communication sites. Similar functions are integrated into surface ships, ground vehicles, and personnel units (see Figure 4.8-1). Each of these platforms provides a set of capabilities that can be further combined for progressively larger and more complex operations.

Technology advances have created expanding demands for spectrum allocation; new spectrum has become available as reliable, inexpensive microwave, and millimeter wave devices, capable of operating at higher frequencies were developed. However, frequencies above 3 gigahertz (GHz) are highly susceptible to atmospheric interference and environmental losses caused by rain or foliage. Based on current technology and propagation limits, the upper range of the spectrum has reached its practical limit.

Because the propagation of electromagnetic waves is a physical phenomenon not limited by political or social boundaries, avoiding unintentional interference with wireless information systems in other countries is mutually beneficial. International and national regulatory processes control access to spectrum. Spectrum is a national asset governed by civil authority. Although standards for spectrum use vary among nations and regions of the world, economic and commercial markets, which are boundary neutral, are often the top considerations in determining spectrum allocation policy and use.

In the past, the prime drivers in Military system design and procurement were technical capability and operational requirements. In that era, as new systems were designed, spectrum use and availability were assumed. Those are no longer safe assumptions. Both Military technology transfer and industry research have accelerated the expansion of



Figure 4.8-1—A wide variety of spectrum-dependent systems are integrated aboard Navy/Marine Corps platforms.

commercial/private sector wireless technology. Every product, device, and system under development must now be open to locating in any spectrum band. The specific portion of the spectrum used determines performance capability, and the equipment and systems using it. The physics of waveform performance drives spectrum desirability. Within the current realm of technology, 6 GHz and below is considered prime spectrum “real estate” due to its propagation characteristics. As technology innovations occur, DON dependence on spectrum access will also increase.

The challenge in today’s spectrum environment is to maintain an appropriate balance of priorities in providing for the needs of all spectrum users. The explosion of spectrum-dependent technologies will no doubt continue, even in the face of a finite spectrum resource.

IMPLEMENTATION

The DoD is exclusively assigned less than 1.4 percent of the RF spectrum to accomplish its warfighting mission. The DON remains an accountable steward for their portion of this national asset. Within the DON, responsibility for spectrum management is vested at multiple organizational levels and in several operational, research, and acquisition areas.



Figure 4.8-2—The DoD is exclusively assigned less than 1.4 percent of the RF spectrum.

Pursuant to the Title 10 responsibilities of the Services to equip their respective forces, the DON maintains its own spectrum allocation management organization (see Figure 4.8-3) and provides a representative to the Interdepartment Radio Advisory Committee. The DON is responsible for granting frequency allocation for equipment and coordinating its use both in the United States and in foreign countries. This involves obtaining frequency certifications and assignments from the National Telecommunications and Information Administration for operations in the United States, and coordinating with host nations through the Joint Staff Military Communications Electronics Board for operations outside of the United States.

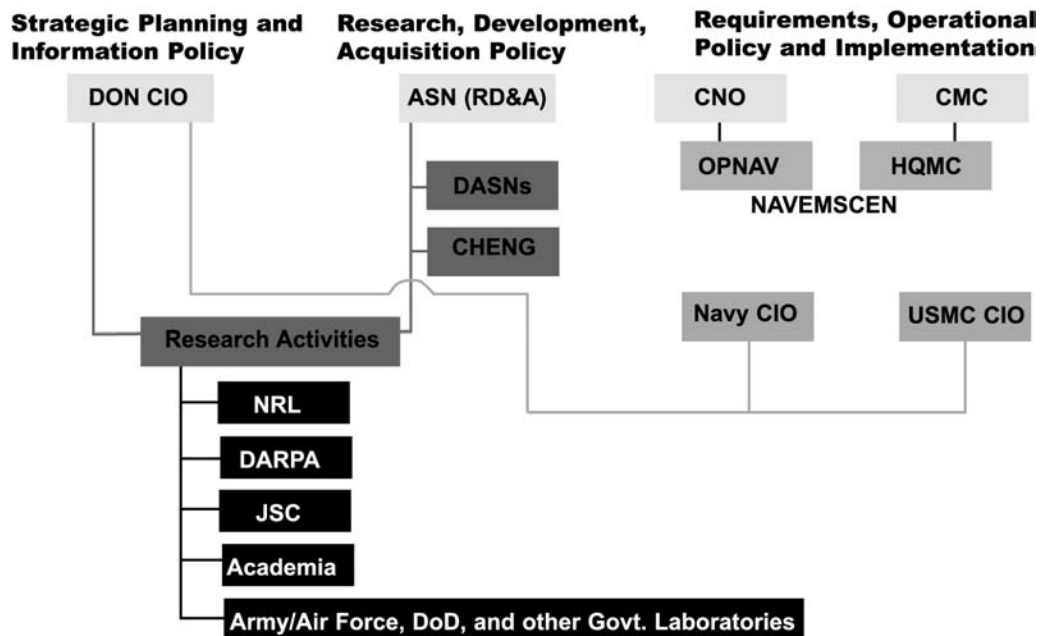


Figure 4.8-3—The Navy has established a Spectrum Allocation Management organization.

The DON CIO's role is to ensure compliance with the DoD spectrum policies, and develop the DON policy and strategic planning for spectrum use. The DON CIO is the DON point of contact for spectrum policy issues and works with industry as the Navy/Marine Corps liaison. The DON CIO supports spectrum analyses and studies with organizations such as the Center for Naval Analysis, the Naval Postgraduate School, the Office of Naval Research, the Joint Spectrum Center, and the Navy Studies Board. The

DON CIO collaborates with the Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN (RD&A)) and the Navy and Marine Corps CIO to develop strategy planning for efficient spectrum use and development.

ASN RD&A monitors compliance with spectrum policy in all phases of the acquisition process. That office ensures that spectrum use and availability is considered in normal programmatic activities. As the DON's lead in research and development, the Assistant Secretary is actively engaged with government research agencies, industry, and private research institutes seeking to leverage new technologies to improve spectrum efficiency and decrease reliance on spectrum.

The Chief of Naval Operations, Space, Information Warfare, Command and Control and the Marine Corps Assistant Chief of Staff have primary responsibility for identifying requirements that support the Navy and Marine Corps operational missions. In their dual role as their respective Service's CIO, they are responsible for implementing spectrum policy guidance. They issue updates to Secretary of the Navy instructions in support of spectrum identification and certification policies for all DON programs and DON-controlled/managed joint programs. The Chief of Naval Operations and the Commandant of the Marine Corps issue operational guidance for the management of DON specific and shared spectrum, control of electromagnetic interference, and they resolve operational issues.

As Naval Forces deploy, Combatant Commanders negotiate spectrum access with host and surrounding nations. The differing spectrum allocations abroad place a premium on frequency agility in Navy and Marine Corps operational systems to adapt to foreign environments. Active collaboration with other Military Services, the DoD, Federal Government, international spectrum groups, and foreign governments is paramount in the DON's ability to effectively and efficiently manage the Navy and Marine Corps spectrum allocation requirements.

The DON has a global electronic networking architecture, Information Technology for the 21st Century (IT-21), to provide seamless, interoperable transfer of voice, video, and data between afloat and ashore forces. Spectrum allocation remains the key to exploit IT-21 capabilities to:

- Reach-back to pull required information.
- Exchange/distribute wideband information.
- Process large volumes of information.
- Implement reliable, jam-resistant communications and information warfare protection.

DON SPECTRUM ACTION AREAS

The DON has identified five spectrum action areas: Policy, Strategic Planning, Operations, Acquisition, and Research and Development. These five areas are components of achieving the vision of an innovative, entrepreneurial, long-term spectrum management strategy based on evolving Naval warfare requirements.

Policy

The Secretary of the Navy is developing technical, business, and operational guidance for proactive spectrum management. The DON goal is to develop a realistic and dynamic Strategic Spectrum Plan that defines spectrum requirements consistent with emerging technologies, commercial trends, and increasing market demands. Development and implementation of the plan will require participation by all DON spectrum organizations and activities. The DON must continue to ensure that the Department has the most effective representation possible in international spectrum negotiations.

The DON will provide ongoing spectrum guidance for program development. Primarily, the DON must continue to ensure all spectrum dependent systems have complete certification reviews at development and acquisition stages to identify and assign required frequencies prior to expenditure of funds.

The Secretary of the Navy will establish a process by which the Navy and Marine Corps can seek the most efficient use of spectrum. This activity will include identification of inefficient systems for transition or planned obsolescence.

In order to provide qualified Navy and Marine Corps spectrum managers, the DON will establish standard operating procedures for spectrum management and support Military and Civilian personnel assignment qualifications.

Strategic Planning

The DON's information needs and its spectrum requirements strain current DON spectrum allocations. To support its strategy, the DON is a major user of commercial satellite communications, cellular telephone, and mobile services. As advanced capabilities are developed to counter emerging threats, spectrum requirements are projected to grow as well.

Faced with these challenges, the DON spectrum strategy identifies and proactively manages the following spectrum allocation issues crucial to the DON operational capabilities of today and requirements for tomorrow:

- Develop and implement a short-term, mid-term, and long-range spectrum vision and strategy.
- Track industry developments in spectrum research and implementation of techniques for more efficient use of spectrum.
- Collaborate with other services to develop a coalesced and symbiotic spectrum plan.
- Provide integrated strategy for system sunset, relocation, and reallocation of spectrum for thorough efficiency by exploiting advanced technological projects, envisaging warfighting requirements and hostile environments into future time intervals, and joint service cooperation to field common systems and share spectral allocations.

These strategies must embrace and foster innovation and business partnerships with industry to encourage the development of new public and private technologies.

Operations

Sophisticated electronics systems operating in a constrained area (such as an aircraft carrier) place heavy demands on the spectrum to accommodate information flow without mutual electromagnetic interference. Navy and Marine Corps defensive and offensive detection, tracking, and weapon systems also place heavy demands on the management and use of the electromagnetic spectrum. Operational forces must continue to be educated and trained on the technical aspects of efficient spectrum use, e.g., shared bandwidth, filter usage, and power usage.

The DON must identify technology to reduce bandwidth needed for control and instrumentation of test and evaluation. Additionally, the DON must seek spectrum consistent with increased instrumentation and test complexity for test and evaluation and training facilities.

Improvements in modeling and simulation data to facilitate the analysis of electromagnetic environmental effects and deployment coordination are necessary. Additional automation to track host nation spectrum usage agreements is an administrative requisite.

Acquisition

The DON will ensure the appropriate use of spectrum by considering new and upgraded systems throughout the developmental process. Spectrum compatibility evaluation models developed early in the system development process will facilitate environmental analysis. Spectrum efficiency must be a priority in system development programs. Spectrum conservation and efficient use will be a metric for program managers. All new and upgraded systems (including commercial off-the-shelf equipment) will account for their spectrum use and impacts based on Military capabilities and spectrum efficiency. Spectrum management requirements will be addressed throughout system life cycles. As a final check, test and evaluation will include ensuring that the system meets certification criteria. Coordination and certification rules must be enforced to avoid spectrum chaos, both within the U.S. and abroad. Spectrum allocation management must be a conscious consideration from system conception through system deployment.

Research and Development

The DON should maintain its preeminence in identifying and evaluating new techniques for efficient spectrum use that could potentially benefit the Navy and/or the Marine Corps. Spectrum sharing and software programmability are compelling technologies whose research and development have benefited from DON sponsorship. Further investment is needed to fully evaluate and exploit emerging technologies such as coherent tracking, orthogonal concepts, and adaptive bandwidth management. ASN RD&A will continue to theorize the practical application of promising science to the warfighting needs of the DON.

Technology advances are allowing DON to use spectrum more efficiently and effectively in the areas of frequency, time, space, and modulation. Once fixed by hardware, operating frequencies are now becoming software programmable over wide frequency ranges. One example is the Joint Tactical Radio Systems which can “sniff” for channels in use and change in near-real time to unused channels, thus eliminating interference.

CONCLUSIONS

Effectiveness in 21st Century warfare will depend heavily on how well the different branches of our Military can communicate and coordinate their efforts on the battlefield.

Joint operations no longer infer just inter Service and traditional treaty partner participation. Now Navy and Marine Corps warfighters must operate effectively with ad-hoc coalition members and international partners for peace. Additionally, the DON must provide its forces the ability to support national security by active participation in homeland defense.

Demands for spectrum to handle the rapidly increasing information flow of modern, Joint, dispersed forces are escalating rapidly. The DON recognizes that Military capabilities must drive spectrum requirements. Spectrum management no longer exists just to prevent electromagnetic systems interference. To ensure uninterrupted, successful, and effective employment of US Navy and Marine Corps operational capabilities, the DON will continue to transform its approach to spectrum management.

Information dominance is key to the success of future U.S. Military operations. Spectrum access is the enabler for that information dominance. The measure of spectrum management success is simple—Navy and Marine Corps warfighters must have seamless and transparent access to spectrum.

4.9 Technology Enablement Strategies

We are inundated with technology solutions for requirements we haven't thought of. Where do new solutions fit into our Enterprise, and how can they contribute to our mission?

—Rick Therren, Technology Enablement Strategies Team Leader

BACKGROUND

The Technology Enablement Strategies concept started back in 1992, at the dawn of the Information Age. Terminals still accessed applications and the PC was an adjunct, agile machine used for offline processing. Offline means processing and massaging data exported off the mainframe to make fancy viewgraphs using pictures and figures keyboarded into programs like WordPerfect and Harvard Graphics.

People in the Department of the Navy (DON) couldn't talk to each other from an information technology (IT) perspective; making information flow electronically was just too hard. The Navy ran 20 different e-mail products. It required a degree in Computer Science to send an e-mail message to an office three rooms down the hall because it went through five e-mail systems, seven Local Area Networks (LANs) and two Wide Area Networks (WANs) to get there. Then, users themselves needed full technical knowledge of the programs, LANs, and WANs before they could use the system. The DON was neck-deep in mainframes, terminals and PCs.

This scenario, repeated throughout the Federal Government, was a result of organizations acquiring and building their own self-contained systems. Knowledge was sinking beneath all of this procured system complexity—and Congress was concerned. The Clinger-Cohen Act of 1996 brought discipline into government IT acquisitions. These acquisitions had to add measurable value to an agency's mission and fit into their enterprise architectures. The Chief Information Officer (CIO) was charged with setting policy to ensure interoperability.

Internet Time

By the time Clinger-Cohen went into effect, the world was moving on "Internet time" and technology stocks were strapped to Saturn Five rockets taking the economy and people's imaginations to the stars. Personal computers broke the one hundred megahertz barrier. It had taken the fifteen years prior to 1996 to get that far from one megahertz. PCs were shipping with a whopping 16 megabytes of RAM. Around that time people were starting to see the effect of Moore's Law, indicating that computers would go faster than people ever needed them to go.

The World Wide Web was at the end of its second generation. Hardly anyone noticed the first generation. Academia and scientists built and used the Web to publish research papers where a text-only browser running on old UNIX systems was the only way they

could access those documents. It was a lot more efficient than the old Network File System because the Web could mask the details of the UNIX file system from the reader. The second generation of the Web came with a new browser (at first just the same old UNIX systems) that could depict rich text, graphics, images, and tables instead of just plain text. In addition, it had a new forms feature offering users the opportunity to send data back to the host via forms—in short, moving from pure consumption to interactivity. Web sites were popping up everywhere.

New software and hardware manufacturers started to build Web solutions for people who wanted something but were still unsure why they needed it. Consumers were buying all sorts of these solutions hoping that they would meet some nebulous and dubious need, while they figured out what they really needed from the Web.

This concept of Internet time brought rapid turnover in technology not seen in the previous years of the Information Age. The Department was still in the mode of buying new technology to patch, replace, or augment systems. As the pace got faster, purchases became even more erratic. The DON struggled to keep pace with change, but it was impossible to keep up. The pace and direction were set purely by technology, and that was changing by the minute.

Meanwhile, the Department was developing its first Enterprise information architecture. This was no small undertaking since organizations within the DON already had architectures for their pieces of the Enterprise. Since the DON is loosely structured to support agility, each sub-organization within the Department has tremendous latitude and fiscal authority, including the acquisition and life cycle management of its IT systems. Bringing all of the nearly autonomous organizations together to agree on a large, detailed Enterprise architecture was time consuming—much slower than Internet time.

While we were negotiating among ourselves over an Enterprise architecture, IT purchases abounded in an effort to keep up with the latest technology. When the first DON CIO came into office, it was recognized that the Department must manage Internet time or it would drain the Department's resources before an Enterprise architecture could be implemented.

IMPLEMENTATION

Understanding the problem was an experience that would take nearly three more years. In the meantime, an initiative was created to begin making a difference using all the understanding the DON had gained up to that point in time.

The concept of Red Teams, comprised of highly skilled IT professionals and engineers on alert, was introduced in early 1997. It was envisioned that the DON would need a comprehensive understanding of emerging issues related to IT on very short notice. The first Red Teams were completely ad hoc and usually worked for an organization within the DON. They typically investigated computer security issues like viruses or unstable operating systems, and eventually also began to support Information Assurance. The part of the Red Teaming that was supposed to look at new technology was harder to get

underway. While Naval Research Laboratory (NRL) performs applied research in areas that eventually find their way into commercial off-the-shelf (COTS) technology, they do not necessarily look at the latest shipping COTS technology. So the Department needed another means to focus on this new COTS technology.

Halfway through 1998, the concept of a Red Team was modified by forming a team within the DON CIO called Leading Edge Services. Leading Edge Services focused on issues related to systems already in use in the Department. The DON had purchased, installed, and operated a multitude of Web sites, content management systems, office automation software, and messaging software. Leading Edge Services recognized that IT purchases were often being made to fill specific needs instead of using existing software to satisfy these requirements.

While the organization has changed since 1998, this modified concept of a Red Team was preserved and given the opportunity to find its place not only within the CIO organization, but within the Enterprise.

CURRENT AND FUTURE STRATEGIES

Today, Leading Edge Services has evolved into Technology Enablement Strategies and is focused on adopting commercial solutions into the Enterprise to fundamentally change the way we use and interact with information technology. Several examples of new technologies that Technology Enablement Strategies is currently reviewing are described in the first two examples below. The third example includes a discussion of work underway that will significantly change the concept of the computer, and the fourth example expands on strategies for learning and collaboration.

Example One: Application of Hard Tokens

Hard tokens are short for Cryptographic Hardware Tokens. A hard token is a digital credential provided by a well-trusted authority and stored on a smart card. The identity on the token is formed using Internet standards and stored in such a way that makes it difficult to steal or misrepresent. These identities are intended to be recognized and usable systems that enable a user to present his or her identity to any system and be authorized to use it at the system's discretion.

Previously, each system maintained its own list of users and used custom password schemes to authenticate them. This meant there was a password for each system to which a user needed access. Hard tokens provide a way for systems to forego their maintenance of users and passwords and rely on a third party that maintains a high confidence in the authenticity of identities so that one source can be used by all applications.

This new technology fundamentally changes the way the DON does business. The Department can begin to move seamlessly through systems while being more secure than before. Processes and information can now flow through many systems. People begin to focus more on the information than the systems that contain it.

Technology Enablement Strategies is looking at how best to get applications and systems to rely on hard tokens. Originally, hard tokens were deployed to identify users to Web sites, and sign and/or encrypt e-mail messages using a personal computer that can process hard tokens stored on smart cards. Unfortunately, that does not cover all the methods used to get work done, nor does it cover all the devices a person may use. It is also necessary for a network to recognize hard tokens because a network operating system maintains all the access control lists not held by discrete applications. Access control lists represent the users' need-to-know. The hard token represents the user and the level of access, but until the user can present his token to a network, the network can't match him up to his need-to-know.

Matching the user to the network can be accomplished in one of two ways. The current way is to use middleware on a workstation that recognizes the user's token and forwards his network password on to the network. This gives the appearance of being authenticated to the network with the token, and it was a good first step. Still, the network relies on the password and not the token, with the middleware acting as an intermediary. The alternative way is to remove the middleware and have the network log the user on relying directly on the hard token. The Technology Enablement Strategies team installed and operates a network using live subjects (in this case, the DON CIO staff) to provide the CIO with first-hand knowledge of the intricacies involved, and to illustrate the best way to achieve network logon with hard tokens.

Example Two: Wireless

The original intent of hard token usage assumed everyone was using a PC. In the past two years, industry has introduced us to the world of wireless computing. DON is not inexperienced with wireless; in fact, the DON is the biggest user of wireless communications in the world. What is indeed new is the introduction of wireless technologies to the user. The DON's use of wireless in the past had been for long haul communications among systems. With wireless technology now in the hands of end-users, DON has the means to change the way people work. With desktop computers, you have to be at a station to feed or consume information. Wireless brings the systems to where work is done, whether a conference room, the flight line, the inventory control point, or even on a bench while waiting for a shuttle to take you from one place to another.

It takes an understanding of industry's offerings to know exactly what it takes to make information more accessible using wireless technology. Technology Enablement Strategies is keeping up with local area wireless standards, wide-area wireless standards, and devices that use either local or wide-area protocols to communicate.

Local area wireless uses a new standard adapted to the old, venerable Ethernet standard. Ethernet is the popular name for IEEE 802. Wireless Ethernet piggybacks onto wired Ethernet under the standard IEEE 802.11. Ethernet is the world's most dominant and economical method for transporting Internet Protocol (IP). With Ethernet extended to the airwaves, there is now a very inexpensive way (today's street price is about \$99.99 per end-point) to extend the IP of the airwaves. Wireless Ethernet is very efficient and fast, making it easy to deploy on small devices such as handhelds. Handheld devices can attach

themselves directly to the local area network (LAN) and communicate directly with the network like a PC does instead of requiring a PC to act as an intermediary using custom hot sync methods. This means a user can take a small handheld device with him wherever he needs to work, all the while being connected to his LAN. Because this is wireless in the local area, coverage is only line-of-sight from where the wireless access point is physically connected to the LAN. Inside buildings, that can mean as little as one hundred feet. Outdoors, it could be as far as 12 miles.

Wide-area wireless has been around since the day of the beeper. More recently, two-way wireless has been sold by telephone carriers such as Cingular and Motient, but it is very slow compared to local area network speeds. Slow speed combined with battery technology and the voice-centric nature of the carriers meant that meaningful two-way wireless just wasn't practical. Today, carriers such as Voicestream are deploying a technology developed in Europe called General Services for Mobile (GSM). GSM can carry a data service called General Packet Radio Service (GPRS). GPRS is a big improvement in speed and efficiency. These technologies are considered evolutionary vice revolutionary to existing, second generation methods; hence the term "2.5G." It is incrementally better than the second generation, but not a revolution in wireless. Still, wireless devices such as handhelds can use 2.5G to consume and manipulate information in a useful manner. And, because they are wide-area, we now have the capability to reach back wirelessly to our network from wherever the carrier provides coverage. In the extreme case this can mean that a user could be on the East Coast connected and communicating with her home network located on the West Coast.

Example Three: Wearable Computers

Some of the more radical areas of information technology research are focused on shrinking and embedding wearable computers into clothing, developing systems that can think, making the computer-user interface transparent, infusing the body's neural network with digital technology, and even harnessing the power of rapid eye movement (REM) sleep for training purposes.

A true wearable computer can be operated hands-free and used while the wearer is moving around. It is always on and has sensors (including wireless communications, cameras, microphones, or Global Positioning Systems) for the physical environment and can convey information to users even when inactive. Wearable devices are predicted to become even smaller and more unobtrusive in the future as components shrink in size. Even the need to carry a battery pack may be eliminated by the Massachusetts Institute of Technology (MIT) Media Lab's research into a shoe that is a part of a personal area network that turns the body into a "wet wire" for transmitting data. This shoe generates power when the user walks on top of flexible film sensors loaded in the soles that generate current by being flexed back and forth (Bass, 1998).

One of the keys to the usefulness of wearables is their ability to display information to the user via a pair of eyeglasses that do not restrict the user's normal vision. Initially developed by the Human Interface Technology Lab at the University of Washington, Virtual Retinal Display devices display what a user would see on his monitor directly on the

retina in a full color, high resolution, wide-field of view screen. The image looks like it's floating in front of the user and the device can be used without a light source (Bass, 1998). With these devices, surgeons could perform image-guided surgery, and maintenance professionals could view manuals and share and coordinate blueprints as they worked.

Andy Flagg, a faculty member of the computer science department at the University of Massachusetts in Amherst is teaching computers how to "notice" a user's routines and offer useful information accordingly. Flagg is interested in how to get a computer to recognize, for example, that if the wearer has entered a conference room at a particular time "it should figure out that I'm going to a meeting and pull out appropriate documents, including minutes of the last meeting, and notes from related discussions" (Luciano, 2000). He is also interested in getting the system to recognize daily routines and provide reminders to the user about tasks that need to be performed. The impact of this type of research on mobile learning can be far-reaching. Imagine prepping an official for a diplomacy meeting by sending all the documents to the wearer's liquid crystal display (LCD) eyepiece or updating the wearer as breaking events happen. The system could also be used during training sessions as a personal coach to remind the wearer to complete tasks in sequence or in a particular way. It would allow one-on-one training to occur without the cost of a team of trainers.

Making the user interface as transparent as possible consumes some scientists and developers in the field of wearable computers. The peripherals they develop run the gamut from the rather mundane (like a forehead sensor that can operate your computer at the blink of an eye) (Bass, 1998) to the more radical (like the US Air Force Human Engineering Division's work on a brain-activated computer-control device that is triggered by reading brain waves) (Bass, 1998). Brain wave reading input devices are not the stuff of science fantasy. Jennifer Healey at MIT's Media Lab has built an affective computer that can read the biometric signals of the user and play music to suit the user's mood and emotional state (Bass, 1998). This system might be very effective for training aimed at changing engrained behaviors or altering unconscious reactions to stimuli that cause stress or fear. Researchers at the University of Rochester are equipped with a virtual reality helmet that is able to recognize key brain signals, and while inside a virtual room, users can turn on appliances by just wishing it so (Sherwood, 2000). While focused on providing physically challenged individuals independence, their research could have significant implications for other industries that need quick response times. Brain-computer interfaces are intent upon making telepathy a scientific reality, and this type of technology, implemented from a central office to a field site via an employee, might result in more efficient communication and a decrease in employee error and misunderstanding.

How is this type of technology used within the workplace to deliver eLearning? Boeing has implemented wearables in their wiring shops. Mistakes in wiring an airplane can be costly, and the wiring complexity previously required assemblers to go back and forth between computer printouts and formboards to see which wire bundles got linked to which connectors. Builders sometimes work with only a single wire at a time, using schematics glued to the boards. Now by wearing a headset with a microphone, voice recognition software, and a transparent eyepiece that works as a display, mechanics are able to access the aircraft manual verbally and have it displayed before their eyes. They can then overlay the

wiring diagram on top of the piece of the aircraft in front of them and with the unit's ability to track the user's head movements, the appropriate schematics zoom into view no matter where the user gazes (Nash, 1997).

Other research institutions have experimented with wearable technology in a range of other industries. Georgia Tech Research Institute (GTRI) for instance, has created two Factory Automation Support Technology (FAST) devices that are being used in the poultry industry by managers who need to monitor inventory without creating paperwork (Sanders, 1999). "(Mobile technology) is intended to support mobile employees as they perform a job, rather than train them before," said Chris Thompson a senior GTRI researcher (Sanders, 1999).

Various research centers are developing systems that will educate the user about their surroundings, as well as provide them essential timely information in adverse environmental conditions. "With wearable technology, it doesn't matter if they're down in a manhole or up in a loft," said Brad Chitty, General Manager of Mobile Communications Services at Bell Canada, in North York, Ontario. "They always have access to customer information as opposed to having to go back to the office or the truck" (Nobel, 2001). NASA's Jet Propulsion Laboratory has developed such augmented reality systems for astronauts. Their prototype, WARP (Wireless Augmented Reality Prototype), can relay to the astronaut her vital signs, the spacecrafts system status and owner manual displayed in an LCD eyepiece, while simultaneously communicating all of her actions to ground control (Britt, 2001). The ability to control troops using wearable technology is currently being demonstrated. Troops no longer need to be within hearing range to receive orders, and Military medics could instantly address health concerns of injured soldiers by reading their biometric signs and locating them with GPS location devices. Soldiers could receive new navigational maps and blueprints within their LCD devices, eliminating the need to regroup to educate the troops on new battle plans, and individual troop movements could be tracked while in the field allowing the commander to maintain control of his team at all times.

Imagine eliminating the language barrier between native speakers of different languages. A 911 operator who gets a call from someone speaking in an unknown language would be able to immediately translate the call and offer assistance in that person's native tongue; or a relief worker would be able to more efficiently meet the needs of those he serves by understanding what was communicated; or a soldier would hear shouts of warning from partner soldiers of another country in a non-native language. With the advances in real-time language translators, all of the above are becoming a reality both through computer-aided textual support systems and through wearable devices that translate and provide real-time language support.

Example Four: Learning and Collaboration Software

Researchers with the Office of the Future Project at the University of North Carolina (UNC) Chapel Hill are working on blending holography, virtual reality, and conferencing to create meeting experiences in which the subjects are viewed as within the same place. On May 9, 2000 the virtual images of a researcher in Armonk, NY and a postdoctoral fellow at

the University of Pennsylvania appeared in a telecubicle set up at UNC Chapel Hill (Lanier, 2001). This type of device allows for physical demonstrations and for the capturing of the actions of the presenter and the meeting members. Like the first transcontinental phone call, the quality was scratchy. It was also jerky, updating around three times a second rather than 10, the minimum speed needed to capture the full range of facial expressions. And it only worked one-way: the people in Armonk and Philadelphia couldn't see Chapel Hill. Nevertheless, it moved UNC video services manager Thomas Cox to say: "It looks like somebody took a chainsaw and cut a hole in the wall and he's on the other side" (Stroud, 2001). Schoolchildren in China, Australia, or Britain could walk beneath massive dinosaur bones in a museum in New York. Patients in remote areas could see a doctor. And once haptic interfaces (devices that react to touch or body movement) are integrated into the technology, people could use "tele-immersion" to come together in even stranger ways. A woman in Europe could reach out and touch her newborn grandchild in the U.S.

High quality tele-immersion will require more bandwidth than what is currently available (e.g., around 1.2 gigabits per second) which leaves the implementation of this type of technology unrealistic—for the time being (Ananthaswamy, 2001). Considering the rate of technological advancements, however, enterprises could be using tele-immersion effectively within the next 15 to 20 years, if not sooner. There has already been preliminary corporate interest in tele-immersion. The McDonalds fast-food chain, showed interest at one early workshop. Says Tom Defanti, one of the researchers from the University of Illinois at Chicago, "McDonalds envisioned fitting tele-immersion booths in its restaurants so people away from home could have dinner with their family. The technology for that is not that far off" (Ananthaswamy, 2001).

There are other virtual solutions to holding meetings for geographically dispersed employees. Subjects involved in the CAVE (Cave Automatic Virtual Environment) at the University of Illinois at Chicago are able to interact with virtual objects by wearing lightweight stereo glasses. Imagine flooding your workspace with a CAVE or tele-immersion set up which projects an off-site trainer into your office. Currently, haptic sensors are being developed that would allow you to reach out and feel the sensation of a handshake with your remote collaborator (Barbian, 2001). These types of technologies could be very beneficial for just in time training for surgical procedures and trauma surgery training when the expert physician is miles away.

Various research centers have expanded upon the concept of transparent computer-user interfaces and have explored how truly transparent systems could be ideal for training purposes. Research at Stanford University has demonstrated that while the dreamer's muscles become temporarily paralyzed by the REM cycle, the physical activity in a dream exhibits the same neural impulses in the brain that the user exhibits when awake. Interested in harnessing this dreamtime for training, the Lucidity Institute has invented a device called the NovaDreamer that professes to send a subject into a REM state by alerting the subject's brain when he/she is dreaming (Barbian, 2001). "Research on how to cultivate peak performance suggests that lucid dreaming may prove to be an ideal training ground, not only for athletics, but also for any area in which skill can be developed," Dr. Stephen LaBerge's Stanford University researcher writes in *Exploring the World of Lucid Dreaming*. Within REM sleep, students would be able to rehearse and prepare for real-life experiences.

Just imagine being able to conduct training sessions to a slumbering class of students—with “dream link technology” computer sensing devices that link an entire class over a “dream network” (Barbian, 2001).

Even more radical than utilizing lucid dreaming as a training ground is the research being conducted by the Artificial Life Team at British Telecommunications in Ipswich, England. Their reports discuss the development of an “immortality chip” called the Soul Catcher that would be implanted somewhere behind the eye and interface with the user’s neural network, creating a truly digitized environment (Barbian, 2001). This type of a peripheral would overcome the difficulties of power supply and the impact of adverse environmental conditions. This system would be able to record what the user thinks and sees and download that information to a mainframe computer making the user a human information machine with an unlimited memory and flawless recall, eliminating the need for a trainer entirely, and ushering in a new world of true human/cyborg entities.

By combining wearable computing with transparent computer-user interfaces and “thinking computers,” the future workplace may become an environment where training is an ongoing affair that is tailored to the individual through devices that will judge how and what to teach an individual by monitoring the student’s movements and brainwaves. Trainers will appear holographically and students will be able to virtually touch them and other objects within a virtual training room. Employees in industries that require just-in-time learning will don LCD eyeglasses, microphones, and other wearable peripherals along with their uniforms each day, and their instantaneous learning will be driven by the experience as suggested by a computer that is monitoring the user’s movements or the supervisor in the control room half a world away. Or in the far distant future, employees will have embedded computers that are run off of the body’s electrical current and will record everything the user reads, hears, or sees. Recording a human experience requires a lot of processing and storage space—more than computers currently have. A human brain is estimated to have “the processing power of around one thousand million million operations per second (one petatops) and a memory of 10 terabytes. If current trends continue, computers could match those capabilities by 2047” (Bell, 1997). Experiences demonstrated in the popular movie, *The Matrix*, therefore are not so far fetched; and it is possible that in fifty years, learners will simply plug in to upload new information, or with current advancements in biotechnology, perhaps swallow a pill to learn how to navigate that new terrain, or speak in German, or fly a plane.

Focus On eGovernment

- 5.1 *eBusiness*
- 5.2 *Knowledge Management*
- 5.3 *Naval Libraries and Information Services*
- 5.4 *Enterprise Portal*
- 5.5 *Knowledge Taxonomy*
- 5.6 *Smart Card*
- 5.7 *Records Management*

INTRODUCTION

The Internet has changed our world. Organizations have embraced the power of the Internet to increase productivity, reduce costs, improve quality of life, and enable fundamental change in the way people work and think. Financial institutions have developed online banking solutions that reduce their cost per transaction by one hundred fold over the cost of a traditional visit to a teller at a branch office. Traditional “brick and mortar” retailers have had to redefine their sales strategy to compete with the successful Web-based retail strategies of companies like Dell Computers and Amazon.com. Major competitors in the automotive and aerospace industries band together in digital marketplaces for a common good without giving away competitive advantage. In fact, the digital revolution has expanded far beyond traditionally information technology (IT)-savvy corporations. Cemex, taking advantage of dashboard computers and Global Positioning System (GPS) receivers, has recast its strategy for delivering concrete in Mexico; reducing costs, increasing productivity, and ultimately improving customer satisfaction.

In a single issue of a national newspaper, fifteen stories appear on how the Internet and information technology have changed the world. These stories describe a broad range of efforts, from organic farmers to custom casket manufacturers using the Internet to display and sell their wares. A casino installs slot machines that allow customers to e-mail other patrons, make lunchtime reservations, and book a tee time, without having to leave the casino floor or even momentarily stop feeding their coins into the machines. Over 60 percent of American churches operate Web sites, and a pastor is quoted as saying that in the past his message only traveled one hundred feet back through the sanctuary, but now his message can be heard instantaneously in one hundred countries around the world. What a powerful statement on the promise of the 21st Century.

eGovernment is “enabled” government . . . government of the people, by the people, and for the people in a virtual world—a collaborative government where technology meets human creativity, and where government manages and shares its vast stores of knowledge with, and for the benefit of, the citizen.

Information technology is being successfully used as an enabling force to replace cumbersome, labor intensive paper processes with “electronic” solutions. Initial strategies, which focused on electronic commerce or “eCommerce” functions such as purchasing and payment, have now expanded to eBusiness and eGovernment strategies that embrace virtually every functional area within an organization. In the Department of the Navy (DON), the foundation for this transformation is being laid through deployment of the Navy Marine Corps Intranet (NMCI). Through the power and reach of a single network, the Department’s personnel will be securely connected in ways never before possible. Imagine the Department’s intranet as a modern superhighway, replacing the old stop light laden, two-lane thoroughfares with a multilane interstate highway system. The opportunities to move information rapidly and securely are tremendous. But at the same time the highway is being built, the Department must also focus on building “fast cars”—applications and systems that can maximize the value that the highway system offers. By bringing together the information superhighway and a fleet of self-service, transaction-based applications, our “drivers”—Sailors, Marines, and Civilian employees deployed around the world—will reap the full benefit of the Internet age.

Knowledge management (KM) is a lynchpin of the Department’s eGovernment strategy. The Department has been recognized in the Federal Government, and indeed internationally, as a leader in the implementation of knowledge management. Dow Chemical describes knowledge management as “providing the right information to the right decision-maker at the right time, thus creating the right conditions for new knowledge to be created.” Through building information repositories and portals that support people, and identifying and connecting authoritative data sources, the Department is promoting the flow of the best information to decision-makers. Real-time collaboration, the growth of communities, and aggressive education and training are transforming DON employees into knowledge workers. As knowledge is shared, the organization learns and grows, and solutions never before imagined become commonplace.

Knowledge management is being embraced across the Department of the Navy, and has made particularly strong inroads among deployed forces in the operational world. Department of the Navy Knowledge initiatives such as Collaboration at Sea and the Knowledge Wall are allowing Carrier Battle Groups to collaborate in real time, reducing cycle time and improving the ability to make complex decisions and address rapidly changing threats.

The Military’s knowledge management programs are so comprehensive, in fact, that the private sector can learn much from them, from more effective ways to apply information technology to new ways of teaching.

Gary H. Anthes in
—COMPUTER WORLD August 21, 2000

The realignment of the policy and coordination for management of Naval library and information services with the Chief Information Officer (CIO) brought the DON CIO's most experienced knowledge workers onto the information management/information technology (IM/IT) team. This marriage changed the role of librarians in the Department, challenging them to embrace rapidly emerging and evolving IT to improve and develop entirely new delivery methods.

A successful eGovernment strategy must also focus on the development of Web-enabled applications and the creation of a single Enterprise portal. The Department of the Navy's Enterprise portal will allow employees access to the intellectual capital of the entire Department. Individuals will be empowered by the knowledge that they will be able to garner, and improvements in productivity will be dramatic. Rather than searching for "best applications," there will instead be a "transparency of applications," as functionally-oriented services are seamlessly provided to users through a variety of channels that allow for access from the office, at home, while traveling, or using a wireless personal electronic device. An Enterprise portal will also allow the Department to achieve substantial cost reductions as redundant legacy systems are eliminated and commands are no longer relegated to only using locally developed solutions and Web sites.

With connectivity and access to data and information, it is essential to provide decision-makers with a clear and easy method to find what is needed at any given moment. The key to success is to organize information in the way decision-makers think about it. DON has undertaken this difficult task through development of an Enterprise Knowledge Management Taxonomy to serve as the common framework for effective user access and interactions. The Enterprise Knowledge Management Taxonomy bridges KM and IM by using both sets of design and architectural precepts to build a classification scheme that is both logical and hierarchical, and centered on intuitive knowledge mapping of the user.

In embracing eBusiness, the Department has taken a number of important steps to be a Federal leader. The Department of the Navy was the first Federal agency to conduct an online reverse auction. Using Internet technologies, reverse auctions allow companies to bid down the price that they are willing to provide to the government for products and services. The first five reverse auctions conducted by the DON produced cost savings of between twenty and thirty percent, and this technology will continue to be used across a broad range of purchases to drive true competition. The Department's eBusiness strategy focuses on transformation. Commands are encouraged to take advantage of the moment of opportunity that the introduction of new technology provides, to reinvent business processes as part of their change management strategy. The Department has also created an eBusiness Operations Office to serve as an innovation center to help activities develop eBusiness solutions, leverage advances already made elsewhere, and develop ongoing partnerships with commercial solution providers.

The DON has also been recognized as a Federal leader in the deployment of smart card technology. For over seven years, the Department has issued smart cards to Navy and Marine Corps personnel at its recruit training centers and elsewhere to improve productivity, enhance quality of life, and enable eBusiness solutions to be deployed in areas such as food services, access control, tool issuance, and medical and dental care. With the

advent of Public Key Infrastructure (PKI) and the ability to carry digital certificates on a smart card, the entire Department of Defense is embarked upon a two year plan to issue smart cards to every active duty, selected Reservist, Government Civilian, and on-site contractor personnel. PKI digital certificates are the foundation for secure eBusiness transactions, and smart cards really are becoming “your passport to the eWorld.”

All of these efforts will allow the DON workforce to become truly mobile, leveraging advances in secure wireless solutions to conduct self-service transactions anywhere, anytime. But the greatest outcome of this eGovernment transformation will be bringing the power of the entire DON shore establishment to our Sailors and Marines, deployed “in harms way” around the world. The mechanic on the ship deployed in the western Pacific can collaborate in real time with the engineer in Crane, IN, who developed the part that she is trying to repair. The surgeon on the aircraft carrier can conduct procedures via telemedicine with the National Naval Medical Center in Bethesda, MD. Someday, a deployed Marine will be able to “reach-back” to Fort Detrick or the National Institutes of Health for assistance in identifying the potential presence of an unknown biological agent. There are a number of challenges to creating an eGovernment environment, many of which center on the organization’s ability to embrace cultural change. However, proactive leaders, willing to take that first step toward transformation are, rewarded by the vast array of opportunities that will result from the leap into the digital age.

5.1 eBusiness

“The eBusiness transformation of the Department of the Navy will significantly reduce overhead costs and improve support to the warfighter.”

—Rob Carey, eBusiness Team Leader

BACKGROUND

The Department of the Navy (DON) has embraced Electronic Business (eBusiness) as the singularly most important tool to modernize, streamline, and reduce the cost of operations associated with our business processes and systems. Implementing eBusiness concepts across the Department will directly and significantly improve service to the warfighter.

There are as many definitions of eBusiness as there are authors on the subject. The Department of Defense eBusiness/eCommerce Strategic Plan defines eBusiness as:

“The interchange and processing of information via electronic techniques for accomplishing transactions based upon the application of commercial standards and practices. Further, an integral part of implementing eBusiness is the application of business process improvement or reengineering to streamline business processes prior to the incorporation of technologies facilitating the electronic exchange of business information.”

Though a vanilla slogan, this definition well captures the essence of eBusiness. It accurately assigns technology to an enabling role while placing first emphasis on process improvement. One must be careful not to interpret “accomplishing transactions” too narrowly. Electronic business is not simply concerned with procurement-centric transactions. Rather, eBusiness applications encompass every facet of the Department’s managerial functions and processes including logistics, training, financial management, supply chain management, health affairs, and personnel administration.

Many businesses and government organizations have successfully implemented a variety of eBusiness solutions leading to significant improvements in process efficiencies, product support, and customer responsiveness. Technology research analysts predict that by the end of this decade, the use of advanced eBusiness processes will be the norm rather than the exception. The term “electronic business” will likely disappear as eBusiness precepts and applications simply become the new way of doing “business.”


IMPLEMENTATION

The DON vision for eBusiness is to create an environment throughout the Department, both afloat and ashore, where eBusiness-enabling technologies, best business practices, and Web-enabled applications facilitate end-to-end operations, resulting in far greater efficiencies in accomplishing every warfighter and mission support function. These efficiencies or savings will be available to reinvest in DON priorities.

eBusiness is defined as the interchange and processing of information via electronic techniques for accomplishing transactions based upon the application of commercial standards and practices. Further, an integral part of implementing eBusiness is the application of business process improvement or reengineering to streamline business processes prior to the incorporation of technologies facilitating the electronic exchange of business information.

The DON Chief Information Officer (CIO) is charged with the responsibility to execute the Department's vision of an eBusiness transformation. Accomplishing such a daunting task requires focused leadership and sufficient resources. The DON CIO put these factors in place through a variety of means. The CIO established an eBusiness team to develop the vision and strategy, and a Department of the Navy eBusiness Operations Office, with a primary mission of helping commands with eBusiness transformation. The new team, along with other Departmental eBusiness leaders, instituted a program of eBusiness pilot projects that invests funds in short turnaround initiatives that "prime the pump" of eBusiness activity across the DON. The CIO consistently emphasized that process improvement is central to successfully applying eBusiness applications. The CIO helped create a forum to take advantage of the synergy of eBusiness efforts underway across the Department. Details of these endeavors are fully described in the ensuing paragraphs.

DON CIO eBusiness Team and Strategic Plan



In February 2000, the DON CIO formally created a dedicated eBusiness Team to develop and champion Departmental policy and strategies to lead the Department's eBusiness transformation (eTransformation). One of the first actions of this team was to write and issue the Department of the Navy Electronic Business Strategic Plan 2001–2002. This plan delineates the mission, vision, goals, and objectives of the Department's eBusiness transformation. It also discusses the concepts of electronic business, delineates the statutory and policy requirements for the eBusiness transformation, and describes eBusiness systems that are already improving Departmental business.

Of particular note, the plan's guiding principles succinctly encompass the primary precepts required for a successful electronic transformation. Those principles are:

- Reengineer business processes as a precursor to applying eBusiness technology solutions.
- Advocate using commercial eBusiness concepts, technologies, and best business practices to improve our business processes.
- Support and promote, with other DoD agencies, an efficient, flexible, reliable, cost-effective eBusiness infrastructure.
- Use commercial applications, standards, and practices as much as possible.
- Employ Web-enabled solutions to transform our Enterprise.
- Develop and maintain eB-knowledgeable teams throughout all of its functional areas.

DON eBusiness Operations Office



To support commands with these and other eB challenges, the DON CIO worked with senior Departmental leadership to create an office with the knowledge and resources needed to provide transformational assistance. As a result, in September 2000, the Secretary of the Navy signed the charter establishing the DON eBusiness Operations Office.

The DON eBusiness Operations Office, located at the Naval Supply Systems Command in Mechanicsburg, PA has two primary missions. One is to be the Department's center for eBusiness innovations. To this purpose, the office acts as a clearinghouse for eBusiness best practices, maintains a catalogue of industry and government eBusiness initiatives, conducts market research, assists planning and organizing transformational activities, provides eBusiness-consulting services to DON organizations, and manages the eBusiness pilot program that provides funding and high level leadership for eBusiness initiatives. The second mission is to provide centralized program management for Departmental card and electronic transaction systems.

The eBusiness pilot program is a "venture capital-like" effort designed to "jump start" promising eBusiness initiatives throughout the Department. These initiatives are limited in scope and require 90 to 120 days to complete, but they directly address Departmental business requirements. Once successfully completed, the sponsoring activity is responsible for formal implementation of these projects.

Over 400 applications were submitted in response to the initial pilot program announcement. Eight pilots were selected for the FY 2001 program. These initiatives covered a wide range of eBusiness applicability. They use the Internet and/or other technologies to improve arranging household goods shipments, manage afloat navigation chart allowances, remotely monitor conditions within storage containers, and automate the completion of confidential financial disclosure forms.



Medical Appointments on the Web, is a joint pilot initiative of the DON eBusiness Operations Office and the Naval Medical Center, San Diego, CA. This project is a Web-based tool that allows clinic staff to schedule multiple appointments for their patients before the initial appointment is even concluded. Further, the appointments tool integrates seamlessly into existing clinical systems that lacked this functionality. Currently, patients schedule specialty appointments by visiting the clinic in person, navigating an understaffed call center, or waiting for mail notification. This tool increases patient satisfaction and convenience while also ensuring efficient and effective access to care. Medical appointments on the Web has recently been selected for DoD-wide use.

The GATOR Link pilot, executed by the USMC Advanced Amphibious Assault Vehicle (AAAV) program, successfully demonstrated the use of telecommunications and Internet technologies to reduce costs, improve responsiveness of the Navy Supply System, and increase combat readiness. It achieves these goals through the rapid exchange of data between contractors, commercial suppliers, and government organizations. GATOR Link

demonstrated online spare parts ordering, Internet technical manual updates, repair before failure diagnostic sensors, and live voice and videoconference between onboard mechanics and remote engineers.

Balanced Scorecard

Under the predicate that if you can't measure it, you can't manage it, the eBusiness Team employed the Kaplan Norton Balanced Scorecard (BSC) methodology to measure the Department's eBusiness transformation. The BSC is an industry best practice that selects measures, which can be easily communicated, to help align the efforts of individuals, teams and organizations to achieve common goals. Typically, these measures track performance across the objectives in four organizational perspectives: financial, internal processes, innovation and learning, and customer. In the public sector, a fifth perspective, stakeholder, is often included given the nature of governmental hierarchy. Measuring and then managing to these objectives helps translate strategy into action.



In Spring 2001, the eBusiness Team formed a working group to “build” a DON eBusiness scorecard. The group was comprised of relatively senior representatives from both functional area management and claimants throughout the Department. This group mapped the Department's eBusiness objectives to the BSC framework and developed initiatives that would assure attainment of those objectives. Then, team members conducted structured interviews with many of the Department's most senior leaders to elicit their opinions in order to develop measures and initiatives for the objectives the leaders judged most important. The interview results were transformed into the DON eBusiness Balanced Scorecard, with short-, medium-, and long-term measurement targets. The resultant scorecard guides the Department's eBusiness transformation and demonstrates how eBusiness investments are supporting the DON's eBusiness objectives, a first in the Federal Government.

Reverse Auctions



An early initiative of the new team demonstrated how eBusiness processes could accomplish better business. In May 2000, the Naval Supply Systems Command (NAVSUP) conducted the first online reverse auction in Federal Government history, in which companies competed online for a Federal contract. The Naval Inventory Control Point, NAVSUP's largest field activity, received offers via the Internet from three pre-qualified suppliers for ejection seat components in U.S. Air Force aircraft. Using secure Internet-based technology, bidders competed in real time for the contract by lowering their prices as they watched their competition's bids. In this instance, the Navy achieved savings of 28.9 percent over the previous historical price for these items. The auction lasted 51 minutes, and the contract was awarded within an hour of the reverse auction closing. In contrast, standard procurement contracts are awarded on the basis of written sealed bids or competitive proposals that routinely require weeks. Subsequent reverse auctions have resulted in similar savings and shortened contract award times.


Process Improvement

eTransformation for an organization the size of the DON is a multifaceted and difficult endeavor. In most cases, locating the requisite technology is the smallest challenge. The Department's complex mission, infrastructure, and global presence complicate even the best-designed processes. Exacerbating the challenge is the fact that many existing processes and systems were built incrementally. This is why process improvement is the most critical component of applying eBusiness precepts. Automating existing manual systems or applying new technology to a complex legacy system may provide an incremental enhancement, but it won't return the large improvements potentially available through a properly designed process.

The level of process improvement applied to transformational efforts varies with the situation. It might be as straightforward as streamlining or modifying an existing process. It could involve thoughtfully combining several sound processes. On the other hand, the situation may require a full business process reengineering effort. In any event, it is essential that proper process design precede the application of new technology.

DON eBusiness Stakeholders' Forum

One key to the DON's successful eBusiness transformation will be to ensure that a synergistic effect results from the Department's diverse and widespread eBusiness efforts. To this end the CIO eBusiness Team and the eBusiness Operations Office jointly formed the DON eBusiness Stakeholders' Forum. The mission of this group is to communicate and



exchange eBusiness information, foster collaboration on eBusiness initiatives, support the implementation of eBusiness solutions, and provide the analysis and input required to help shape and influence the Department's eBusiness strategy.

The Forum meets about four times per year. Membership is comprised of senior DON officials from a variety of commands and activities charged with oversight or implementation of eBusiness initiatives. This seniority level is desired so that members can directly influence the course of eBusiness at their commands. Everyone who participates has a voice in setting the Department's course in eBusiness.

THE FUTURE

The DON CIO, along with the eBusiness Operations Office, will remain at the forefront of leading the Department's eTransformation. These offices will continue to foster innovation, identify leading best practices, support commands on their eBusiness journeys and, in general, champion the enormous return on eBusiness investment.

Similarly, together the Department's eBusiness Strategic Plan and the eBusiness Balanced Scorecard guide and monitor the Department's eTransformation. Both the Strategic Plan and Scorecard will be periodically updated as eBusiness best practices develop, as new technology enablers arrive, and as initiatives are completed.

The two offices are working together to define the best portfolio of eBusiness processes and technologies. Such a portfolio identifies and prioritizes technologies. It also provides guidance on evaluating and selecting eBusiness investments. A portfolio assists commands in spending their funds most effectively. Further, by providing a list of the most promising technologies, a portfolio helps to reduce the prevalence of both disparate systems that can't interface with one another and duplicate initiatives that waste scarce resources in redundant efforts.



One goal of the eBusiness Operations Office is to be the Department's "one-stop-shop" for eBusiness assistance and knowledge. The office developed and promulgated a communications plan to ensure DON personnel are aware of the wealth of available expertise. A new Web site, the Knowledge Exchange Gateway, will provide a single source for eBusiness consulting services, eBusiness knowledge, and idea sharing.

The eBusiness Pilot Program, very successful in FY 2001, will continue with an even greater number of short-term, high-impact projects. First round eBusiness pilot projects selected to receive funding in FY 2002 include "Unit Level Performance and Readiness Prototype Web Site," for the Naval Warfare Assessment Station, Naval Surface Warfare Center (NSWC) Division and "eFacilities Support Services," for the Naval Facilities Engineering Command Headquarters. eBusiness efforts will continue to flourish, and the Department of the Navy will evolve to a true eGovernment organization, where the "e" not only stands for "electronic" but also for "enabled."

A SUCCESS STORY



As stated earlier, eBusiness is not just concerned with procurements and supply related transactions. eBusiness is applicable to every facet of the Department's managerial functions and processes. An excellent example is the Dental Common Access System (DENCAS) that provides Navy Dentistry with a world-class eBusiness system. DENCAS provides enhanced data management through a secure, Web-accessible central data repository. This was accomplished by consolidating patient and productivity data from approximately 400 stand-alone databases resident in Navy Dental clinics around the world. Previously, the clinics submitted paper feeder reports that headquarters personnel entered by hand, into the central legacy system. In turn, paper reports from that system were mailed to dental clinics and other commands. DENCAS directly improves the overall dental readiness and health of the DON.

The system provides Navy and Marine Corps line commands the ability to monitor, in near real time, their dental recall, readiness, and health status from their own locations. Further, they can view or print recall and readiness reports at their discretion. Previously, commands managed their dental status with the paper reports generated and mailed by the dental community. This new capability assists the line commands in maintaining readiness at a higher state than with the old paper-based system.

DENCAS allows the dental community to examine and evaluate Navy-wide dental treatment needs and dental productivity through the Web-accessible data repository. This enables the dental community to evaluate future dental manpower requirements and conduct treatment needs trend analysis. DENCAS also assists in evaluating current manpower assignments based on workload needs and productivity data.

The Web-based design of DENCAS allows efficient configuration management. Because DENCAS is not resident on client workstations, system changes are accomplished via access to the server. Web server design offers the benefits of decreased maintenance cost, improved access to the application, and the ability to protect patient data.

5.2 Knowledge Management

Knowledge is actionable. The value of knowledge lies in results.

—Frank Sowa, Enterprise Knowledge Team Leader

The historical landscape of the Department of the Navy (DON) information technology (IT) world was built on presence: obtrusive technology with hardware and software controlled at the local level. IT decisions were made in a vacuum, the same vacuum that reinforced the stovepiped, crisis-driven activity that tried to make sense out of the encroaching information chaos. Learned people searched for a standardized, stable environment. As the knowledge age dawned somewhere in the late 1990s, a quite-different vision of the future began to emerge. People began to rely on virtual resources, trading stability for invisible technology and flexibility. The word ubiquitous came into its own, trailing on the heels of a recognized need for open standards and interoperability. The concept of “continuous learning” became a necessity in order to keep up with the incredible technology changes occurring daily. And “information needs” were being redefined as “knowledge needs.”



Knowledge Management (KM) champions were emerging throughout the Department of the Navy, positioned at varying levels of the Enterprise. While they were focusing on their organizational areas of responsibility, there was an unspoken common message: *There is something here of value. Knowledge management offers an opportunity for us to do what we do better.*

The importance of Knowledge Management is clearly stated in the DON Information Management/Information Technology (IM/IT) Strategic Plan, provided to Congress in June 1999. Goal 4 of the plan calls for implementation of strategies that facilitate the creation and sharing of knowledge to enable effective and agile decision-making. Recognition of this imperative, with knowledge management tied directly to mission performance, is demonstrated in the Knowledge Centric Organization Model published by the DON in April 2000. The words were clear: Knowledge management offers the potential to significantly leverage the value of our IT investment and the intellectual capital of our people. Information technology and information management are essential, but alone are insufficient to achieve information superiority. To achieve this, knowledge management strategies facilitate collaborative information sharing to optimize strategic and tactical decisions, resulting in more effective and efficient mission performance.

Knowledge management can be viewed as a process for optimizing the effective application of intellectual capital to achieve organizational objectives.

KNOWLEDGE SUPERIORITY

With the energy building toward KM implementation across the DON, the Navy Department led the charge to figure out just what the new world of knowledge meant in terms of the Military forces. A Knowledge Superiority Project workshop, held at the U.S. Naval Academy in Annapolis, MD, brought together senior Military and Civilian personnel for six intensive days to focus on this important area.

Knowledge Superiority means achieving sustainable competitive advantage over our adversaries. Building on the integration and interoperability of our warfighters, it is characterized by tactical and technical competence and cohesive teams. It includes capabilities for knowledge management, effective information operations and network management, as well as organizational relationships that encourage the sharing and creation of knowledge. This translates into superior knowledge of the battlespace and the ability to rapidly bring overwhelming force against our adversary.

At the Knowledge Superiority Project workshop, the sixty plus participants shaped the vision for the Department:

More than any other nation, more than any other Navy, and more than ever before, we rely on the creativity, ingenuity, and intellect of our people. As we cross the threshold of the Information Age, we intend to realize this awesome potential in every corner of our Navy, by every person, as a highly interactive total team. Transcending even our current advantage in physical firepower, our Navy will be alive with the fire of shared understanding. We will do this because we must for our Navy's relevance and readiness in this new era. No foe, present or future, will match our knowledge or our ability to apply it. Indeed, just as forward presence has become a way of life for us, so too will Knowledge Superiority become a Navy way of life.



The Stennis Battle Group provides an example of Knowledge Superiority in action: In the Pacific Fleet, the Stennis Battle Group led development of a KM system providing rapid, flexible, robust collaboration, planning, and execution of all Carrier Battle Group operations. Collaborating at sea is difficult. There is limited ability to connect a large group of worldwide users to a massive amount of widely-distributed information via narrow and intermittently connected channels with sufficient speed and accuracy to facilitate tactical and strategic decisions. The Fleet must deal with varying IT systems and capabilities, such as ship type limitations, bandwidth variance, a mix of legacy systems, and software version lags. There is also great variance in the type of data transferred, including: operations, weather, air warfare, order of battle, and intelligence-related data. Data varies in format, protocol, security classification, and national language. In addition, multiple personnel (Commanding Officer, Tactical Action Officer) must have the same view of some pieces of information to support tactical decisions, and some data must be restricted so that only authorized personnel may view it.

Battle Groups have struggled with the ability to capture, archive, and later access key data and unique processes associated with repetitive operational deployments. Historically, there have been issues with reinventing the wheel on each cyclical Battle Group deployment. The bottom line is, it has been almost impossible to efficiently transfer and leverage knowledge.

The Stennis Battle Group initiative used commercial off-the-shelf products to ensure industry standards and leverage the industry investment, and planned an instantaneous, context-oriented communications capability with audio, video, and application sharing. This successful and scalable project was defined, developed, and installed in 42 days with a team of seven people. Recognizing the value of this KM approach, the Atlantic Fleet quickly began adopting it for use in all their Battle Groups. For this groundbreaking work, the Stennis Battle Group Carrier Group 7 received a knowledge sharing award for “Most Scalable KM Solution” at the DON Knowledge Fair 2000.

BUILDING THE FRAMEWORK

The high-level Department definition of knowledge management views KM as a process for optimizing the effective application of intellectual capital to achieve organizational objectives. To appreciate the intent of this definition requires a discussion of the Department’s understanding of “intellectual capital.”

Intellectual capital covers the broad spectrum from tacit to explicit knowledge loosely framed through a discussion of Human Capital, Social Capital, and Corporate Capital. Human Capital, the Department’s greatest resource, is made up of an individual’s past, present, and future knowledge and competency. Each person brings a unique set of characteristics and values from the past, including expertise, education, and experience. Built on these characteristics and values are a set of capabilities and ways of seeing and living in the world (such as creativity and adaptability). Just as important is a person’s future potential. Part of the success in asymmetric warfare is for leaders to have the capacity to learn and quickly respond to emerging challenges.

Social Capital includes human and virtual networks, relationships, and the interactions across these networks built on those relationships. It also takes into account all the aspects of language, including context and culture, formal and informal language, and verbal and non-verbal communication. Also added to this grouping is an element of patterning that deals with timing and sequencing of exchange, as well as the density and diversity of the content. In short, how much, how often, and how intense.

Corporate Capital, sometimes called Organizational Capital, includes intellectual property, and corporate functional and organizational processes. It also includes all the stuff in databases, all the stuff we can visibly get our hands around, all the stuff that has been made explicit. The challenge of the Department, then, is to fully leverage its intellectual capital through sharing, collaborating, innovating, and learning within the framework of its needs for security and information assurance.



DON sees information technology, information management, and knowledge management as connected layers built upon a strong, supportive infrastructure. Each successive layer must be in place to successfully implement the next layer, yet the full value of the layers cannot be achieved in today’s knowledge economy without success throughout all four levels. That means there needs to be good Information Management to effect good KM, and good IM, in turn, is dependent on the right technology investment. Intuitively, the Department has known that using

information to create knowledge to drive improved decision-making was the ultimate IT goal. Knowledge management has provided the framework to make that intuitive knowledge explicit.

The capital elements that drive the DON definition of KM can be traced through IM, IT and the infrastructure (see Figure 5.2-1). For example, *Social Capital aspects of IM* would focus around relationships; *Social Capital aspects of IT* would center around connectivity; and the *Social Capital aspects within the infrastructure* are very much concerned with the use of teams. Following the KM concept through these four layers surfaces critical focus areas that individually and collectively affect the success of the system.

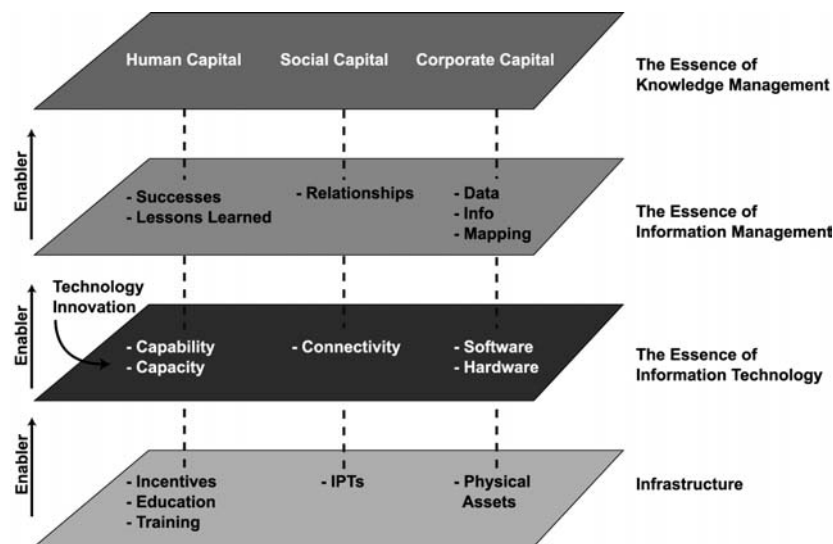


Figure 5.2-1—The Department's definition of Intellectual Capital includes all the elements of Human Capital, Social Capital and Corporate Capital.

At the tactical level, DON has developed a knowledge management implementation framework built around five balanced concepts: technology, content, process, culture, and learning (see Figure 5.2-2).



The important aspect of balance is to ensure the Department doesn't go down one path without bringing in the others, i.e., technology alone is insufficient, it is necessary to simultaneously change processes and provide tools for people to use that technology. In like fashion, it is critical to locate and achieve the point of equilibrium for the dynamic tensions arising through implementation of knowledge management systems. How much risk are we willing to take to achieve leverage and, conversely, how much leveraging are we willing to do despite the risk? How much data and information is it better to leave at the local level, and how much should be available globally? How much data and information—and what data and information—should be made explicit? How much data and information—and what data and information—should be captured in a formal system? In this world of access and excess, the answer is not automatically "more."

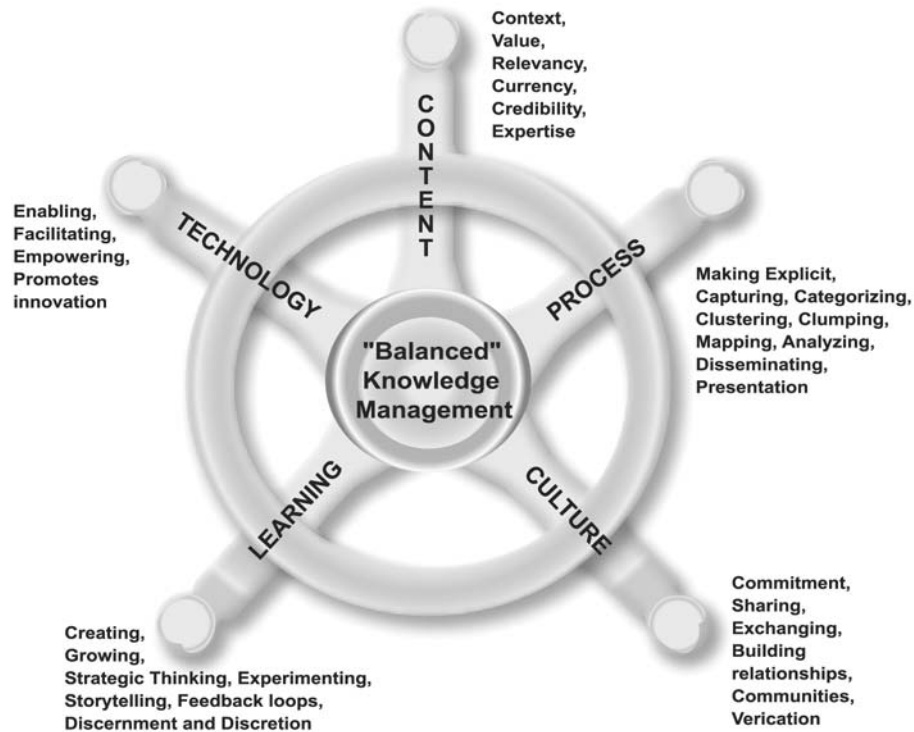


Figure 5.2-2—In the KM Implementation Framework keywords are provided to stimulate thinking about the system or process being implemented.

In each of the five areas of Figure 5.2-2, a few key words are included to stimulate thinking. This figure serves as a template to ask the critical questions that, when answered, will help create a true knowledge system. Several emerging concepts represented in this figure bear a short discussion.

Context. Knowledge management has brought focused attention to the importance of capturing the context along with information and knowledge artifacts (information that has supported the creation of knowledge but is stored as information). Context is unique at any given point in time. It is based on environmental factors, human interactions, recent events, and potential future actions. Knowledge systems must capture the context along with decisions. This can be done in a number of ways. For instance, a special context field in a database can record important environmental factors that might easily be lost when the decision is looked at down the road. Or, a short video clip of the decision-maker talking about the reasons a decision was made could be included with support material.

Clumping and clustering. Clustering is when you bring data and information together that is similar or related, i.e., first and second cousin organization. This process of categorization by similarities is the current popular approach to organization of data and information. It supports ease of locating specific data, and can lead to innovation and insights. Clumping is driven by decision-making. You figure out the decisions you need to make at the top levels and dig out, down, and around to find the authoritative data fields you need from disparate locations. Then you link directly to those fields for continuous

real-time feed to support your emerging decision-making requirements. The organization of information and knowledge around key decision points, closer to that of the human brain, can increase the efficiency and effectiveness of decision-making.

Decision Grounding. Historically, the Department of the Navy has placed significant emphasis on grounding decisions with explicit data, and verifying those decisions through evidence, documents, and references to prove truth and accuracy. Yet, in the complex world of today, captains of ships and managers of support organizations are often called upon to rely on their “gut” feelings. For this reason, grounding decisions on implicit data has become more important. This grounding is achieved through verification, the process of consulting a trusted ally to ensure the reasonableness or soundness of a decision.

Discernment and Discretion. If only two words come to the fore in implementation of knowledge management, they are discernment and discretion. Taken together, these terms address the concepts of selection, valuing, and laying aside, i.e., the ability to identify and choose what is of value, and the equally difficult ability to toss aside that which is not of value.

The framework in Figure 5.2-2 can be used as a template to impose over a KM system or process. In this manner, it suggests the questions that need to be asked to achieve success. Questions can be asked at the key word level, or, ultimately at the key concept level: How does this system/process fully exploit technology? How does it ensure the right content? How does it streamline processes? How does it facilitate individual, team, and organizational learning? How does it enable cultural change?

Storytelling. The construction of fictional examples to illustrate a point, can be used to effectively transfer knowledge. A variety of story forms exist naturally throughout organizations, including scenarios—the articulation of possible future states, constructed within the imaginative limits of the author, and anecdotes—brief sequences captured in the field or arising from brainstorming sessions. Scenarios provide awareness of alternatives and are often used as planning tools for possible future situations. To reinforce positive behavior, sensitive managers can seek out and disseminate true anecdotes that embody the value desired in the organization. The capture and distribution of anecdotes across organizations carries high value. Dave Snowden, a consultant and author in Great Britain who has investigated the use of storytelling in organizations for the past dozen years, has discovered that once a critical number of anecdotes are captured from a community, the value set or rules underlying the behavior of that community can be determined (Snowden, 1999).

Conveying information in a story provides a rich context, remaining in the conscious memory longer and creating more memory traces than information not in context. Therefore a story is more likely to be acted upon than normal means of communications. Storytelling, whether in a personal or organizational setting, connects people, develops creativity, and increases confidence. The use of stories in organizations can build descriptive capabilities, increase organizational learning, convey complex meaning, and communicate common values and rule sets.



The former Under Secretary of the Navy used stories to help Congress visualize the value the Navy Marine Corps Intranet (NMCI) would add to the mission of the Department. One story conveyed how Petty Officer Storm, deployed aboard the USS San Jacinto, was able to reach-back via NMCI to the telemaintenance expert at the Naval Surface Warfare Center in Crane, IN, to quickly resolve an equipment failure. Another story tells about the possible presence of a biological agent detected by forward-deployed Gunnery Sgt. Jackson. Jackson uses NMCI to link back to the Centers for Disease Control in Atlanta, GA and Ft. Dietrick, MD, to contact the experts who analyze the threat and download appropriate procedures. Stories are also an integral part of the DON Knowledge Centric Organization Toolkit, which has been distributed across government and industry, worldwide.

With the advent of the Internet and intranet, there is a larger opportunity to use stories to bring about change. Electronic media adds moving images and sound as context setters. Hypertext capabilities and collaboration software invites groups, teams, and communities to co-create their stories. New multiprocessing skills are required to navigate this new world, skills that include the quick and sure assimilation of, and response to, fast-flowing images and sounds and sensory assaults. In summary, when used well, storytelling is a powerful transformational tool in organizations, one that all of our managers and leaders across the Department need to utilize.

STRATEGIC IMPLEMENTATION

With approximately 800,000 employees, the Department is learning how to take a holistic, distributed, implementation approach to facilitate success. It is holistic in the sense of focusing on a myriad of value-added activities such as building awareness, identifying KM champions, promoting systems thinking, facilitating Communities of Practice, incentivizing knowledge sharing, and building and providing KM tools. Distributed in the sense of championing from the top to “encourage the 1,000 flowers,” while simultaneously providing tools and facilitating knowledge sharing to leverage the value of successes and encourage a connectedness of choices.

The Navy has gone full-speed ahead in adapting knowledge practices and processes. There is no company in the world anywhere near it in scope.

—Larry Prusack, Executive Director,
IBM’s Institute for Knowledge Management



A core element of this strategic implementation was early development of a Knowledge Management Community of Practice (CoP). The KM CoP evolved from two KM conferences sponsored by the Navy Department in late 1998 and early 1999. These events attracted Knowledge Management champions and innovative thinkers who recognized the opportunity KM could bring to their day-to-day operations. The Navy Post Graduate School in Monterey, CA, facilitated an approach that valued proposed projects in an attempt to begin to understand what was different about KM.

Though few of these proposed projects received direct funding, many of the ideas were implemented within existing program funding. Membership in the DON Knowledge Management Community of Practice now includes over 60 organizations, and is steadily increasing. The Community has a Web-enabled virtual support and exchange system and is actively sharing thinking and best practices (see Section 6.5 “Communities of Practice” for additional information).

To further support this infusion of good ideas and best practices across the Enterprise, the Department is partnering with world-class industry organizations and other government agencies in the Institute for Knowledge Management and the American Productivity and Quality Center. These organizations are doing cutting-edge KM research and provide excellent learning forums for the DON KM Community of Practice.



To share, recognize and incentivize good ideas and best practices, the DON's Knowledge Fairs highlighted DON, DoD, and industry efforts in knowledge management, knowledge sharing techniques, and eBusiness, and the great strides the Navy-Marine Corps Team is making towards becoming knowledge-centric. A highlight of the Fair is the opening ceremony in which the Secretary of the Navy gives remarks and personally presents DON eGovernment awards for knowledge sharing. DON, DoD, and industry exhibitors eagerly discuss their KM and eBusiness projects while enthusiastic attendees learn and network. The exhibits are creative, high-tech, and informative, and demonstrations and speakers are featured throughout the day. The sharing that occurs at the Knowledge Fair continues through the video capture of candid remarks by senior DON leaders and the initiatives exhibited at the fair on a CD, called *A Compendium of eGovernment Initiatives*, which is distributed throughout the DON and other agencies following the Fair.

DON's strategic implementation of KM is built on a Systems Thinking model. The continuing surge of information technology investments over the past few years has significantly increased the amount of data, information, and knowledge the decision-maker has available, thereby increasing the complexity of decision-making. As this complexity increases, we invest in more information technology to help solve the problem, thereby further increasing the amount of data and information, and further increasing, in turn, decision-making complexity. This reinforcing cycle continues. To break this loop, the DON is building balancing loops at the individual, organizational, and Enterprise levels (see Figure 5.2-3).

The inner balancing loop shows that as decision-making complexity goes up there is an increased need for workforce cognitive skills. Systems Thinking is one solution. As we increase our individual skill sets in Systems Thinking, decision-making capability increases, closing the gap between decision-making capability and decision-making complexity. The middle balancing loop shows that organizational knowledge management processes (systems) improve decision-making capability (at the organization level) and the outer balancing loop shows that knowledge portals do the same at the Enterprise level. That's a lot of balancing. The bottom line is that the DON needs to attack the system at every level to take full advantage of this thing called knowledge management. DON tools are being created at all three levels identified in this model.

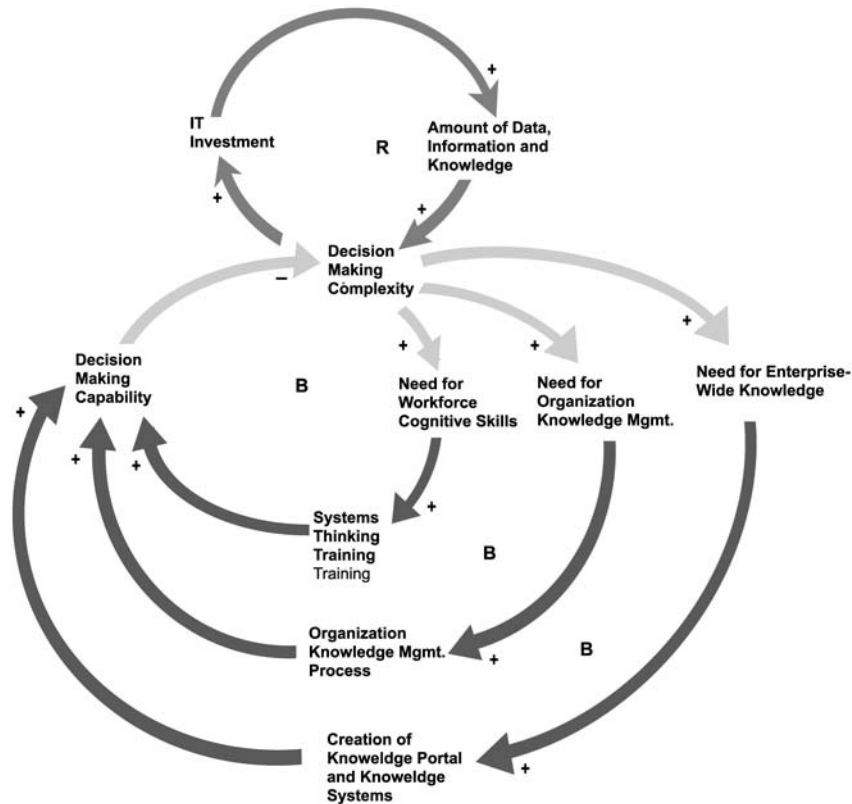


Figure 5.2-3—The DON is addressing KM implementation at the individual, organizational, and Enterprise levels.

Addressing the acquisition of cognitive skills at the individual level is DON's *Systems Thinking* virtual tool. Systems Thinking is one of the five disciplines of the learning organization (Peter Senge, *The Fifth Discipline*). Systems Thinking provides an approach for managing complexity by helping decision-makers recognize and understand the cause and effect relationships among data and information. To do this, it identifies archetypes (or patterns) that occur over and over again in decision-making (see Section 6.2).



To support DON's movement toward becoming a learning organization, the DON CIO promulgated Continuous Learning guidance directing each member of the IM/IT workforce to participate in 80 hours of learning experiences each year. The "Continuous Learning" experience covers a broad spectrum of experiences including mentoring, attendance at conferences and work exchanges, as well as more formal participation in training. It also includes the use of computer-based training and distance learning, utilizing, for example, the Systems Thinking virtual course. Each individual's Continuous Learning implementation approach is developed with his/her supervisor and completion is self-certified in concert with the performance appraisal process. In early 2002 the DON developed its first guidance tool on *Learning in a Virtual World*. In addition, the Department identified roles and developed a career path for knowledge workers (see Section 6.1 "IM/IT Workforce Competency Management" for additional information).

BECOMING A KCO



The *Knowledge-Centric Organization (KCO) Toolkit*, created by DON CIO in 1999, and vetted through the KM Community of Practice, is focused on implementing knowledge management at the organizational level. This tool, packed with templates, case studies, and reference material, leads organizations through the phases of achieving a knowledge-centric organization, providing resources for local decision-making. A KCO is one that (1) learns constantly, (2) facilitates collaboration across diverse opinion, (3) connects people and delivers them the right information at the right time for decision and action, (4) innovates continuously, (5) makes quality decisions faster, (6) reduces product and service cycle time, and (7) accomplishes its mission more productively.

One of the crown jewels of the U.S. Navy's huge knowledge management program is a CD intended to help organizations become "knowledge-centric."

Gary H. Anthes in
—COMPUTER WORLD August 21, 2000



The DON CIO provides a team of experts who visit commands to help them in their journey toward becoming knowledge-centric. KCO Assist Teams help commands organize, plan, and develop initiatives to build a KCO. Assist Teams are available to DON commands to support them in implementing knowledge management (KM) throughout the design, development, and execution of a project. The objectives of assist visits are to train local project teams to become KM experts and share KM lessons learned and best practices across the Enterprise. The three primary tasks associated with the assist visits are: (1) conducting training seminars on KM and KCO methods and principles, (2) assisting with existing KM projects, and (3) developing a KM system that consolidates the interrelated knowledge, information, and data.

For example, an Assist Team worked with the Space and Naval Warfare Command (SPAWAR) Systems Center Charleston for six months to build the organizational, cultural, and IT processes and systems for them to collect, organize, and share critical knowledge assets. A KCO Assist Team is also working with Naval Sea Systems Command (NAVSEA) Keyport where the team is developing a KM system to support a cross-functional integrated view of Underwater Weapons Readiness Indicators. This system will allow Keyport to execute important decision-making and action taking activities with higher efficiency, productivity, effectiveness, and innovation by sharing and reusing critical knowledge from Keyport technical experts. Teams have assisted other commands including the Marine Corps, the Naval Facilities Engineering Command, the Office of Naval Research, and a combined Community of Practice of all the organizations at the Washington Navy Yard.



At the Enterprise level, the Department is working to bring the Navy Marine Corps Intranet (NMCI) into existence, and developing an Enterprise portal and taxonomy to facilitate flow (see “Enterprise Portal” and “Knowledge Taxonomy” later in this chapter). The DON will implement an Enterprise portal concomitant with the NMCI under the direction of the DON CIO. The mission of the Enterprise portal is to provide all DON personnel with one fully customizable, Web-enabled portal into all electronic information assets existing in the DON. The portal must achieve this access by developing global access to DON approved, common sets of applications and authoritative data to support mission accomplishment. Through the DON Enterprise portal, each organizational unit in the Enterprise has a common portal framework with the flexibility to support local users, if required, with the appropriate information resources. At the local level, the command portal aggregates data and facilitates information transactions by bringing local information consumers and producers together. Users are not islands unto themselves; given information in context, they need to take action—often in a collaborative setting. The DON Enterprise portal connects users to leverage expertise, share insights, and implement policy and strategy changes in real-time or through shared databases. The portal will be a primary facilitator of organizational interaction, extending the information portal from a passive information kiosk to a forum for organizational interactions between employees, customers, partners, and other stakeholders.

One of the first knowledge portals in DON was the Pacific Fleet’s Knowledge Homeport. This portal, linking over 200 databases through the Internet, improved productivity through the elimination of non-value activities and promoting the reuse of knowledge. Initial savings of 18,000 staff hours per month were identified.

A Center for Naval Analyses study issued in Spring 2000 looked at over 50 portals, describing their attributes and assessing their placement in a continuum moving from Web-enabled portals to knowledge portals. Attributes that are identified as moving toward the “knowledge portal” concept include collaboration and feedback mechanisms, multiple ways of connecting and presenting data, and tools for building context and creating knowledge. An important learning from this study is that it doesn’t make sense for every portal to embody the knowledge portal concept. More is not always better. Web pages and information portals are intended to meet specific needs and they will reside at some point along the continuum according to those needs.



As the successes of KM in the Department grew, the reputation of DON as a world-class leader in the implementation of KM also grew. The DON model was presented in the keynote address of the first Organization for Economic Cooperation and Development for the European States Knowledge Management Conference in Copenhagen, the DON KM change strategy was keynoted at the Singapore eGovernment conference, and over a dozen allied governments have sent contingents to learn from the DON. The Department has also served for two years as co-chair of the KM Working Groups under the Federal CIO Council, supporting the important work of KM government-wide.

NOW AND THE FUTURE



To date the DON CIO has distributed over 30,000 KCO toolkits worldwide. The demand for this organizational resource continues as other government organizations leverage the best practices and lessons-learned from DON implementation of KM. Other KM resources developed and shared are in the areas of Communities of Practice, Information Literacy, and Learning.

In the Fall of 2001, the DON collaborated with dozens of other government organizations through the Federal KM Working Group to provide the first Federal-level resource on KM. This virtual resource is a compendium of work products developed under the auspices of the Federal CIO Council with contributions that cross historic organizational boundaries. It provides best practices, tools, examples, and a valuable set of resources for fostering and facilitating KM in the Federal Government (see www.km.gov). Development and distribution of this CD provided another step in the government journey to take full advantage of what KM has to offer.

As the DON moves forward in implementing Knowledge Management and ensuring Knowledge Superiority, our knowledge workers will need new skill sets. Moving from an information-centric Enterprise to a knowledge-centric Enterprise, new technologies will continue to emerge. As we uncover the full potential of information management and knowledge management, and figure out better ways to do them, there will be a steady increase of activity in those areas. Then there is an emergent pattern of something called value transformation, which calls for new skill sets for workers in the knowledge economy. These skills include intuiting, integrating, and innovating; sensing, scanning, patterning and synthesizing; judging, storytelling and persuading; and knowing. These concepts are discussed in Section 6.2, "Integrative Competencies."

The continuing Enterprise Knowledge vision is focused on content management, portal structure, collaborative tools and knowledge delivery, and prototyping for knowledge based policy and guidance, as well as knowledge management in its historical sense and team integration. On the horizon are a content management tool, a single DON portal, new collaborative tools and processes, (including expansion of the community concept), and DON guidance and policy to embed all our learning into the future infrastructure.

The future? Data and information will continue to increase exponentially. Knowledge will move into the bottom line of every successful organization. And people will be people, only smarter and wiser, and living in a new knowledge world.

WHAT DOES SUCCESS LOOK LIKE?

Commander McKinney's day is already full of meetings to resolve programmatic issues concerning a special warfare project for which he is responsible. In a quiet moment, however, he recalls the days when preparing and coordinating responses for this and similar projects took months of data gathering, reconciliation, analysis, and option paper development. Now that the Chief of Naval Operations (OPNAV) staff is knowledge-centric, the time to process program plans is reduced to under one-third the time. Just

before heading to his first morning meeting, CDR McKinney checks his voice mail and learns that one of his programs, vital to Seal Team connectivity, is in jeopardy. He asks an assistant to attend the meeting and heads to his desktop where he logs on to the OPNAV operations portal to quickly assemble a briefing package for the Admiral.

Within the portal, McKinney deftly navigates to three sections—the Fleet Commander's operations capability page, the Systems Command financial page, and to the Warfare Development Center's modeling and simulation site. Quickly pulling in the latest capability requirements from the Commanders-in-Chief, CDR McKinney forwards this information to the Development Center's modeling site where he asks a researcher to conduct a rapid analysis on two new options: one that reduces the number of hand-held cellular devices by twenty-five percent and one that tests a new system configuration. While his modeling request is being processed, he ties in to the Systems Command's financial system to obtain the latest project-funding stream—updated within the past twenty-four hours. After breaking down individual component costs, McKinney reaches back to the Development Center's modeling results and generates a point paper comparing capability and cost tradeoffs. At noon, CDR McKinney drops the package off to the Admiral's Executive Assistant and heads to the Pentagon athletic facility to change for a quick run around the Washington Monument.

5.3 *Naval Library and Information Services*

Our libraries are working to provide world-class library and information services for all Naval personnel anytime, anywhere.

—Joan Buntzen, Librarian of the Navy

INTRODUCTION

The innovative alignment of policy and coordination for management of library and information services with information management/information technology (IM/IT) planning and management in the Department of the Navy (DON) establishes a vital connection between Naval libraries (information and service providers), and the information technology infrastructure (networks and systems). With this alignment, the Naval library community has gained access to valuable business experience in Enterprise licensing and higher-level visibility, while IT policy makers and planners have gained insight about content selection, delivery, management, and use. This partnership facilitates developing the right approach for building an effective system of library and information services across the Department.

This is an era of radical change for libraries of all types—public, special, and academic. The possibilities presented by rapidly emerging and evolving information technologies challenge library managers to continuously hone vision, mission, and strategies to improve and re-engineer services, as well as develop entirely new delivery methods. In spite of downsizing and budget constraints, there are opportunities for Naval librarians to share in the benefits of information technology and both anticipate and creatively respond to the changing missions and needs of the organizations they serve. By working cooperatively with the DON Chief Information Officer (CIO) staff, Naval librarians increase and improve information access to all personnel, more cost effectively share the infrastructure, address interoperability concerns, streamline acquisition processes, reduce duplication of effort, develop common standards and practices, increase economic leverage through inter-site licensing, and improve location and use of valuable resources by users.

NAVAL LIBRARIES

There is a long Navy tradition of building library and information services. The Navy Department Library, now located at the Washington Navy Yard, is the oldest continuously operating Federal library. It traces its roots to March 31, 1800, when President John Adams directed its establishment. In 1821, the USS FRANKLIN a flagship on the Pacific station, deployed with a library of 1500 books purchased with funds raised by the crew. Other libraries were established throughout the 19th Century, including the Naval Academy Library; and in 1919 the Secretary of the Navy requested the American Library Association to assist with developing a professionally directed ship and shore library program (now the Naval General Library Program).

Naval libraries and information centers serve a very diverse population of users, including Sailors, Marines, science researchers, engineers, undergraduate and graduate faculty and students, intelligence analysts, health care professionals, attorneys, policy makers, and managers, as well as the general public. Currently, there are approximately 115 special, medical, and academic libraries; 94 general or base libraries; and 300 shipboard libraries. Except for the general and shipboard libraries, there is no centralized resourcing and management of Naval libraries; each command provides funding and support for its local library. Resources and services vary widely, from a very technically advanced and comprehensive digital science library at the Naval Research Laboratory to many one- or two-person libraries providing limited or very specialized services.

Today, Naval libraries are managed and staffed by a cadre of dedicated professionals who are committed to preserving and nurturing the Naval information heritage. They work hard to continuously improve accessibility of collections and services and to be on the leading edge for new innovations. Naval librarians actively participate in Federal, national, and international library science affairs, and have earned national and international recognition for their efforts.

MANAGEMENT OF NAVAL LIBRARIES AND INFORMATION SERVICES

Responsibility to coordinate and align policies for Naval library and information services throughout the DON was transferred from the Naval Historical Center to the DON Chief Information Officer in January 1999. The purpose of this realignment was to integrate coordination of library and information services with DON IM/IT strategy and planning activities to facilitate more effective distribution of and access to information and knowledge resources.

The responsibilities of the Librarian of the Navy include:

- Provide administrative and technical advice to Naval libraries.
- Advance development and implementation of best practices, standards, and performance measures.
- Provide leadership in application of new technologies.
- Develop an information-sharing program to meet present and future requirements of the Department.
- Serve as liaison with governmental and professional organizations and represent the Department on matters of concern for Naval libraries.
- Establish channels of communication and information exchange among library personnel.
- Provide leadership and a central information point for analysis and research on dealing with problems and issues of concern to libraries.
- Develop virtual tools in support of the librarian mission.
- Provide leadership to improve acquisition of resources and services by libraries.

The Chief of Naval Education and Training has overall operational responsibility and provides technical guidance to base and shipboard libraries. Associated duties are carried out by the Naval General Library Program Office, and the director represents this library community in its relationships with the DON CIO and the Librarian of the Navy.

TECHNOLOGY IMPACT ON LIBRARY MANAGEMENT AND SERVICES

New technologies have had significant impact on libraries for improving access and delivery of services. They have also significantly affected the way libraries are organized and managed. Technology applications in library science have created capabilities for delivering new and more comprehensive services, and transforming library organization and management. Managers must constantly review their allocation of personnel and collections resources to deal with the complexity of automated systems (implementation, management, and migration), cost of electronic resources, costs of maintaining both electronic and print collections (as necessary), and developing changing staff skills.

Development of integrated library system software (ILS) in the early 1980s established the capabilities to automate library functions and provide online access to library holdings. These capabilities became the foundation for organizing and building the electronic library or “library without walls.” Today’s ILSs are Web-enabled and allow users to access their library’s catalog from their desktops. Links to content externally or remotely stored can be embedded in the catalog records. Purchase costs of ILS software systems depend upon size and function of the library’s collection and services, but start at about \$60,000 and typically are in the \$150,000 plus range. Due to purchase and maintenance costs, many Naval libraries are not able to purchase an ILS or migrate to current generation systems. Naval libraries use several different commercial off-the-shelf (COTS) ILSs, and only the 17 Marine Corps general libraries share a common or union integrated library system.

Delivery of services to the desktop also places new requirements on library staff. Selection of publications and information resources is more complex and labor intensive due to the range of available products and the need to more carefully evaluate aspects of these products such as interfaces, currency, comprehensiveness, technical support from the publisher/vendor, etc. Information architecture (organization) and enabling connectivity to electronic resources and services is required of library staff since the advent of the Web and intranets, and this expertise is generally not available at current staffing levels in Naval libraries. Digitizing locally developed information resources, often a responsibility of Naval libraries, requires additional hardware, software, and staffing resources.

CHALLENGES

There are many challenges to providing state-of-the-art library and information services. These challenges fall generally in the areas of workforce, costs, organization, and processes.

Workforce. The library workforce has downsized significantly since the end of the cold war due to consolidations and closures of Naval facilities, along with general reductions in the size of the Naval workforce. Only about 50 percent of Naval libraries are managed by a professional librarian (i.e., holding a master's degree in library and information science). Retiring librarians, library technicians, and technical information specialists are not being replaced due to downsizing and budget constraints. (The exceptions are the Naval academic institutions and medical facilities in which library programs and services are requirements for accreditation.) There are no Navy-wide intern or mentoring programs for library personnel.

Costs. The ever increasing and, at times, rapidly escalating costs of information resources is a major barrier in providing quality library services and is a particularly critical issue in science and technology subject areas. For instance, the average cost of a periodical subscription in a technical area was \$638 in 1999. The overall cost of subscriptions in all subject areas has risen more than 200 percent since the early 1980s. With static or no-growth Naval library budgets, this requires continued cancellations and, as a result, collections will continue to shrink in size.

Adding or substituting electronic versions of periodicals (and now, books) is far more expensive than providing just print copies, and some publishers require subscriptions to both. Additional labor costs associated with staff time required to work complex procurement and licensing processes, negotiate with publishers for rights to archives and back-files, rights for interlibrary loan, establish connections, establish authentication and authorization procedures, and instruct users in the use of multiple resources and access paths are also incurred. Libraries with small staffs and budgets are simply not able to participate.

Naval libraries are mostly overhead funded operations, and must be competitive with other organizations in their commands for hardware and software budget resources. In addition, libraries must usually find funding for IT support services. IT costs, coupled with the high cost of publications or content form significant challenges, if not barriers, to libraries exploiting the possibilities of networked information services.

Organization and Processes. Developing Naval-wide library and information services in a networked environment is made more difficult by the lack of resourcing for unified initiatives. Naval libraries are funded to support only the organizations or commands they serve and do not have discretionary funding for joining centralized and multiyear efforts to establish and improve electronic services. Many Naval personnel do not receive badly needed library services, including access to desktop information resources that are cost or subscription based.

There are economies of scope and scale to be realized through resourcing centralized acquisitions of information resources and systems management. This is evidenced by many multi-institutional library consortia in the public and academic sectors receiving regional or local grants, endowments, or seed capital to fund and maintain commonly needed resources and services. The Navy has had some success in consortium procurement and licensing of electronic resources in Navy, but only the larger libraries have the budgets to take advantage

of cooperative buying on behalf of their users. Enterprise or centralized funding, acquisitions and licensing, and systems management are essential to developing global library and information services.

INNOVATIVE APPROACHES

Consortium of Naval Libraries. An inter-command organization of Naval librarians, the Council of Scientific, Special, and Technical Librarians, was established in the early 1950s and met twice a year to exchange information and work on projects of mutual benefit. Although the Council continues, by the mid-1990s, Naval librarians had begun to note achievements in the public and academic library arenas in which libraries banded together to form cooperative buying groups to leverage their content budgets and to consolidate common virtual and digital resources and services. As a result, Navy and Marine Corps librarians met in Dam Neck, VA, in March 1997 to establish the Consortium of Naval Libraries (CNL).

The mission of the CNL is to “facilitate state-of-the-art access to library and information services to all Naval personnel in support of their missions, whether for operational readiness, research and development, situation awareness, decision-making, education and training, or personal enrichment, wherever, whenever, and in an appropriate format.”



The Consortium now consists of approximately 60 member libraries. Members and working groups advise and assist the Librarian of the Navy on matters affecting library services and information resources. The CNL also explores areas of cooperative support and resource sharing and investigates possibilities for leveraged buying and distributed costs.

Licensing Electronic Information Resources. A major motivation in forming the CNL was to aggregate purchasing power of Naval libraries. Beginning as a pilot project in 1998–99, the CNL Procurement Working Group and Librarian of the Navy licensed several commonly needed resources for desktop delivery. In the initial project, five participating sites saved \$150,000 in the cost of resources over what they would have paid had they purchased them independently, and in 2002, a total of almost \$7,000,000 had been saved through consortium licensing. By centralizing the procurement and licensing, the initiative also significantly reduced command library, contracts, financial, and legal costs by eliminating the duplicative efforts. In addition to saving money for CNL member sites, other benefits of consortium licensing include publishers and vendors becoming more knowledgeable about Naval requirements and offering pricing models better suited for our environment. In the current year effort, several resources have been licensed for second year options, locking in prices a year in advance. This greatly helps librarians plan their allocation of funds for electronic resources. For more information on Enterprise licensing, see Section 8.3.

Building the Electronic Library. The first effort to build inter-command virtual library services was the Navy Virtual Library (1997–99) focused on providing gateway desktop access to scientific information resources across the warfare centers and the Naval Research Laboratory. This initiative provided valuable experience, not only in developing a common

interface, but also in developing an approach to distributing costs for expensive resources and services across organizations.

The Navy Marine Corps Intranet (NMCI) presents new challenges, but also exciting opportunities to advance an Enterprise-wide electronic library system. Librarians, especially in the first implementation phase of NMCI, are looking forward to consolidating organization and access to desktop resources commonly licensed under the Consortium initiative. In addition, the NMCI and its common access point, the Enterprise portal, will provide a gateway to virtual resources that are recommended by librarians for relevancy to Naval personnel, as well as a system to alert users to new documents and resources. Consolidating this presentation of virtual resources will save duplication of effort by librarians and facilitate cooperative Web mining and further collection development.

Naval science librarians are working to realize a long-held vision to consolidate access to commonly licensed science journals via the Naval Research Laboratory Library's digital library system, TORPEDO. Several sites are joining in an effort to consolidate licenses to electronic journals published by Elsevier, American Institute of Physics, and the American Physical Society, that are locally mounted at the Naval Research Laboratory. The new digital library initiative will leverage the interoperability objectives of NMCI and provide full information services to the desktop.



Developing User Information Skills. Information Literacy, or the skills today's workers need to locate, extract, integrate and communicate information, is a major concern for librarians. Naval librarians became even more acutely aware of the need to help users develop these skills with the advent of electronic journals, and two years ago formed the Consortium Working Group on Information Literacy. The group worked on collecting marketing and user instructional materials developed by other librarians, and also publisher materials and resources that were available and considered to be particularly helpful. The group is now working with CIO staff to expand this effort and build an Information Literacy toolkit that will help Naval personnel locate, evaluate, and effectively use networked information resources, as well as to self-assess their skills, and to integrate these skills more effectively into their daily work.

CONCLUDING THOUGHTS

These library and knowledge initiatives are critical to success in supporting the workforce today and in the future. Naval personnel serve a global organization and must have connection to information and expertise pertinent not only to their fields of work, but also to continuously enhance their awareness of current events, developments, and trends. Naval libraries endeavor to support this vital connection as well as to preserve the Department's information heritage, but it has become increasingly difficult. Much work needs to be done, and there are areas yet to be addressed, such as developing a successful strategy for small Naval organizations to afford cost-based resources. By centralizing the library management function under the CIO, Naval libraries are better positioned to build cross-organization and Enterprise access to information and knowledge assets for all Naval personnel.

5.4 Enterprise Portal

The Enterprise portal will finally enable the flow of the right information to the right people at the right time without inundating them with superfluous flotsam and jetsam.

—Hun Kim, Enterprise Portal Team Leader

BACKGROUND

There is an immediate opportunity to rapidly deploy a significant information management capability that will provide substantial enhancements to the daily operations and quality of worklife of the Navy and Marine Corps team. Deployment of enterprise portals is commonplace in private industry, and is considered a best practice for enabling knowledge management and collaboration throughout the private sector. Not only is the return on investment quickly realized, but significant strides are made in organizational effectiveness and efficiency. The Hunter Group projects that 85 percent of “Global 2000” companies will have deployed corporate portals by 2003. This approach is also gaining momentum in the government sector; the Army Knowledge Online portal has close to a million users, and the Air Force has deployed their initial portal.

DESCRIPTION OF INITIATIVE

With implementation of the Navy Marine Corps Intranet (NMCI) and Information Technology for the 21st Century (IT-21), the DON has already laid the foundation for deployment of a Department of the Navy (DON) Enterprise portal. This infrastructure will provide every Sailor, Marine, and Civilian in the Department with the hardware and tools necessary to utilize “best of breed” information technology (IT) applications. This investment is significantly diminished, however, without the tool necessary to utilize this infrastructure. Laying fiber optic cable is a worthwhile investment, but unless the cable company is willing to provide digital television programming to the customers, the investment is wasted. The Enterprise portal is the most effective approach to providing valuable content and Enterprise applications to all DON personnel.

The Enterprise portal will provide a single point of access to all DON information management systems, as well as connectivity to other governmental and commercial Web sites (see Figure 5.4-1). The Enterprise portal will also promote Enterprise-wide process reengineering, eliminate stovepipe management, improve productivity, save money on duplicative infrastructure, provide enhanced information assurance, and support retention through improved quality of life and quality of the workplace.

ENTERPRISE PORTAL CONCEPT

Users are not islands unto themselves; given information in context, they need to take action—often in a collaborative setting. The DON Enterprise portal connects users to leverage expertise, share insights, and implement policy and strategy changes in real-time or

through shared databases. The portal is a primary facilitator of organizational interaction. The DON portal extends the information portal from a passive information kiosk to a forum for organizational interactions between employees, customers, partners, and other stakeholders.

The Enterprise portal will serve as a gateway for single point access to all DON information management systems as well as connectivity to other governmental and commercial Web sites.

The role of the Enterprise portal is to integrate services throughout the organization, and to provide additional services for Enterprise portal participants such as quality assurance, data standardization, meta-data management, interoperability, and Enterprise-level information resource management. Portals integrate useful information and capabilities from various sources and present this data in “modules.” Each user can build a personalized view of the Enterprise by choosing the modules to embed in a portal page. These modules bring together Enterprise-wide eBusiness solutions, knowledge management, virtual collaboration, decision-support tools, as well as the entry into each application that users need to successfully perform their jobs every day. Integration lies at the heart of the portal’s ability to access information from a wide range of internal and external information sources and to make it available for display at the single-point-of-access desktop. The required information might be an e-mail, a fax, an image, or the results of Online Analytical Processing analysis. Ultimately, the portal is a network of information that transcends barriers between users and the information systems and applications that support mission requirements.



In the near term the DON CIO is committed to supporting the Department’s Task Force Web initiative. The initial objective is to provide a portal, which will provide access to at least fifty applications maintained by DON commands. The DON CIO is providing the common look and feel guidance for the portal, a new taxonomy and ontology, as well as the initial Extensible Markup Language (XML) schema guidance.

The Enterprise portal will integrate services throughout the organization. Portal functionality is evolving from information access to information management and ultimately to knowledge management. Knowledge and content management will be integrated, and best eBusiness practices leading to workforce efficiencies will be applied to the Enterprise portal. As the Enterprise portal is established, redundant applications and supporting infrastructures will be identified and recommended for elimination. The portal, riding on the existing NMCI, will use single Public Key Infrastructure certified sign-on inherent in the Common Access Card, to ensure security.

The screenshot displays the DON Enterprise Portal website. At the top, a navigation bar includes links for 'InfoStore', 'MyProfile', 'Help', and 'LogOff'. Below this is a search bar with the text 'Adv. Search' and a 'go' button. The main content area is divided into several sections:

- Left Sidebar:** Contains the 'DON Enterprise Portal' logo with the tagline 'EXCHANGE & TRANSFORM'. Below the logo are links for 'Home', 'Local', and 'WorkPlaces'. Further down are portraits and names of key personnel: Secretary of Defense (Hon. Donald Rumsfeld), Secretary of the Navy (Hon. Gordon England), Chief of Naval Operations (ADM Vern Clark), Commandant of the Marine Corps (GEN James L. Jones), Department of the Navy CIO (Mr. Daniel E. Porter), and Vice Chief of (name partially obscured).
- Main Content Area:**
 - Top Section:** A large banner titled 'New Horizons Ahead' with the sub-header 'Web-applications are going to change the way the Navy does business!'. It includes a 'Read Article Below' link.
 - Web-Applications Section:** A text block stating: 'Today, the Navy maintains thousands of applications on millions of computers; the goal for the future is to "web-enable" these applications so users will be able to access them at centralized locations (aboard ship, Network Operation Centers, etc.), from any computer with a web browser. You are now logged into a "Pilot" version of the Task Force Web Enterprise Portal. Many web-applications have already been divided into "web-components" which are accessed by "Service Modules" in this Portal. Web-applications today may have many of these web-components (some duplicative with other applications), and in the future, only the "best of breed" will qualify for "TFWeb Service Modules". The official TFWeb mission is "to provide integrated and transformational information exchange for both the ashore and afloat navy to take full advantage of Navy's IT21 and NMCI infrastructure investments."'
 - Portal Tutorials Section:**
 - 1. Introduction (Mandatory):** Covers Task Force Web history, Internet Portal concepts, and the power of Web-Applications. Includes a '>>> learn more' link.
 - 2. Portal Operation (Mandatory):** Basic operating instructions including description of the Portal Header, Workplace fundamentals, INFOCOM.
 - Official Links Section:** A list of links including Department of Defense, Navy, Marines, DefenseAmerica, DefenseLink, Reserves, Government, FirstGov, The White House, Homeland Security, Health, Finance, Thomas, HomePort Program, TFWeb, NMCI, IT21, and DON CIO.

Figure 5.4-1—The Enterprise portal will provide a single point of access for DON users.

SUPPORT TEAM

A portal integration team will need to provide support for business process development by integrating content, enabling technology, and developing standards. The DON Enterprise portal will comprise Enterprise-wide data management and interoperability meta-data standards to provide the foundation for data interoperability and will help users identify authoritative sources to ensure data consistency among diverse systems. This integration team will also provide guidance, assistance, and methods of operation for Department-wide integration of all Web-enabled or other content. Two key staff elements, collaborating as an Enterprise-wide catalyst and authoritative source for IT integration and change, will be functional area knowledge managers and knowledge engineers. These two groups will work closely with their Fleet equivalents to manage the process for assessment, development, implementation, and evaluation of all DON portal products.

BENEFITS ACROSS THE ENTERPRISE

By using portal technology, Enterprise-wide savings can be achieved. Through an Enterprise portal, DON can provide tools and services to produce savings that could not otherwise be realized at individual Naval commands. Examples of portal-enabled technology enhancements include but are not limited to:

- Elimination of the need to build specific interfaces between legacy applications by using Integration Broker technology at the Enterprise level.
- Use of a single PKI certification processor rather than processors for each application saves not only money but also decreases development time.
- Implementation of other corporate level applications including eProcurement and eWorkforce solutions.

Significant strides have been made in internal corporate workplace portals through which employees can reach personnel, training, operational, and logistics systems. The DON can exploit this technology and savings. The “Enterprise” is the right place for this activity.

BENEFITS TO SAILORS AND MARINES



The portal has the ability and the capacity to enhance the “Quality of Service” of every Sailor and Marine. By providing valuable workplace resources on the Enterprise portal, all DON personnel will look to the portal as the authoritative source for services and information. Examples of services that can be provided to personnel include, but are not limited to:

- 24/7 access to technical manuals, knowledge management based FAQs, and live expert assistance.
- Scheduling/registering personnel appointments such as medical and dental appointments, housing, childcare, and personnel moves, etc.
- Automated check-in/check-out procedures across the Enterprise.
- Telemaintenance, telemedicine, and distance learning.

CONCLUDING THOUGHTS

The Enterprise portal will serve as a gateway for single point access to all DON information management systems as well as connectivity to other governmental and commercial Web sites. Building on a successful intranet approach, deployment and utilization of the Enterprise portal will lead the DON to one of the most significant change management efforts in its history. The Enterprise portal will provide a revolutionary conduit to information that was previously not available to Sailors and Marines on the deck plate as well as the leadership of the Department. Through its proper utilization, the Enterprise portal will help to eliminate stovepiped management, improve productivity, and reduce duplicative infrastructure through the sharing of knowledge and enabling collaboration on topics across distance, job function, and command. By deploying the portal at an Enterprise level, significant savings, both in time and dollars, can be achieved by leveraging the software and knowledge infrastructure across the entire DON.

5.5 Knowledge Taxonomy

Creating an intuitive yet consistent classification framework for all DON knowledge, information, and data will allow all of us to corral our information systems and exploit their great potential to enable greater DON efficiency, effectiveness, and innovation.

—Dr. Geoffrey P. Malafsky, DON Taxonomy Project Partner

BACKGROUND

Achieving Knowledge Superiority, both for the Warfighter and support forces, requires us to capture, organize, and disseminate critical knowledge in a timely and succinct manner. We cannot merely expand access to knowledge, information, and data by building large repositories, since without a clear and easy method to find exactly what people need at any given moment, our forces will continue to succumb to information overload and not achieve the objectives of Knowledge Superiority. The proliferation in the quantity of electronically available information is overwhelming people and network systems, and is making it very difficult for users to find necessary information in the time they have available, especially in knowledge management (KM) systems that strive to deliver answers and targeted links. The key to this success is to organize information according to how users think about it, which often varies from command to command, person to person, and day to day, to facilitate the rapid and precise navigation of huge volumes of potentially relevant material to the few definitely pertinent items.



As part of the Enterprise KM and integration efforts, DON CIO is working with Task Force Web (TFWeb), PEO-IT, Navy Marine Corps Intranet (NMCI), Chief of Naval Operations, Office of the Secretary of Defense, and other stakeholders to design architectural and content management standards and policies to allow all DON personnel to effectively use the wealth of knowledge, information, and data in the DON, both explicitly available in electronic form and the tacit knowledge of our people. This will leverage the vast breadth and depth of our knowledge to achieve greater mission success, efficiency, and innovation.

A key part of this strategy is the methods and tools used to organize and classify the vast volume of knowledge, information, and data throughout the DON Enterprise. DON CIO is coordinating the development of the Enterprise Knowledge Management Taxonomy to serve as the common framework for effective user access and interactions with the NMCI Enterprise portal and the applications Web-enabled by Task Force Web. This taxonomy embodies the best practices and lessons learned in organizing and classifying Enterprise-scale information repositories within the Department of Defense (DoD), Federal Government, and corporations. The Enterprise KM Taxonomy bridges KM and information management by using both sets of design and architectural precepts to build a classification scheme that is logical and hierarchical, as well as centered on users' intuitive knowledge mapping. In addition, knowledge sharing requires the context in which the information was created and will be used, and the relationships among component items.

TAXONOMIES

Taxonomies are the classification scheme used to categorize a set of information items. They represent an agreed vocabulary of topics arranged around a particular theme. Although they can have either a hierarchical or non-hierarchical structure, we typically encounter hierarchical taxonomies such as in libraries, biology, or Military organizations. This type has a tree-like structure with nodes branching into sub-nodes where each node represents a topic with a few descriptive words. For example, the following figure shows a portion of the familiar Dewey Decimal System that was introduced in 1876 as a general catalog of knowledge and is the most common system used in libraries.

Sample of Dewey Decimal System				
600	Technology (Applied Sciences)			
	630	Agriculture and related technologies		
		636	Animal husbandry	
			636.7	Dogs
			636.8	Cats

Figure 5.5-1—An information classification scheme using the Dewey Decimal System.

The need to classify information is not new. One of the first large organized cataloging and classification projects was in the center of ancient knowledge at the Alexandria Library in Egypt. Its first bibliographer Callimachus compiled the *Pinakes*, a 120 volume subject catalog of all the library's books. He is considered the founding father of librarians since he did not just list the books, but included the author, date on the text, and comments on authenticity to guide users (Davis and Wiegard, 1994). However, many others throughout history solved the classification problem by strictly limiting the number of books by religious, political, or economic reasons, and then organizing the set by acquisition date, size, or other simple criteria.

Thus, classifying information becomes more important as the number of items increases and people have more trouble remembering what they have and where to find it. This is now crucial as we buckle under the immense volume of information available to everyone by the electronic networking of the world. We have become the fabled man dying of thirst while at sea as we search for the one or two items that answer our needs from within this sea of information. Indeed, KM is specifically focused on not only giving people the right information, but going to the trouble of distilling it into validated contextually connected knowledge that fuses information and data from a variety of distinct topical areas. When we ask a colleague what the Commanding Officer wants us to do, we don't want to be given the latest PowerPoint presentations or status reports, but rather a direct answer such as, "The Admiral wants us to immediately get the readiness status of the Battle Group for a potential operation tomorrow. We need to contact both the Joint Meteorological and Navy Staff codes to get the newest logistics data and Meteorology and Oceanography (METOC) analysis. If METOC can't accurately predict tomorrow's weather

in the mission area, send out the new Micro-UAV with the miniature covert METOC system and have it feed data directly into the Course of Action and Sensor Performance Prediction systems right up to mission time.” This is an answer that a human gives that does much more than point to the individual reports or Web sites, and allows the questioner to immediately start acting, and deciding their next activity.

A different way to solve this problem is to use automated search engines to find the best information that fulfills a user’s query. This has been a very popular approach in the last few years with the growth of commercial search engine and portal tools like IBM’s Textminer, Microsoft’s Sharepoint, Verity, Convera, Altavista, Google, Ask Jeeves, and Autonomy. Yet, despite their marketing claims, performance metrics collected annually by the Federal Government’s Research and Development agencies, Defense Advanced Research Projects Agency (DARPA), and National Institute of Standards and Technology show that these tools still cannot satisfy user needs on realistically large volumes of dense topic areas. The Text Retrieval Conference results show precision levels of only approximately 40 percent for automatic searches and 60 percent for manual searches (Jones, 1999). It is easy to show why these systems have failed to solve the information retrieval need: a 10,000 item repository (small for Enterprises like the DON) with 10 items directly pertaining to a query requires a 99.9 percent filtering accuracy to deliver these items to the user. Lower values result in either the user not getting the information at all or having the search engine deliver a larger number of lower relevancy ranked items (recall percentage) to ensure that the desired items are in the retrieved set. However, this latter approach, which is the one most often used, forces the user to wade through a large number of irrelevant responses, and has led to high levels of user frustration and disenchantment with these systems.

THE FRAMEWORK



Now that we know we still need to classify information to help sort through the large number of items, the question becomes what framework to use. There are many existing standards from the Federal Government, DoD, consortia, and professional societies. For example, the Defense Technical Information Center has a technology taxonomy that is a standard for the DoD, while the Standard Subject Identification Code (SSIC) is the standard for all DoD information, including memoranda and records management. Similarly, the Library of Congress Classification (LOCC) is a commonly used general purpose system. However, taxonomies inevitably have a central theme that guides how the tree structure is arranged. For example, the LOCC and Dewey Decimal System are built from a perspective of classifying knowledge itself in a general purpose manner. Thus, the major LOCC headings include topics such as: Philosophy, Psychology, Religion, Auxiliary Sciences of History, History (General), and Fine Arts. In contrast, DTIC’s major headings are more focused on technical issues and include: Aviation, Agriculture, Chemistry, Electrotechnology, and Fluidics. Clearly, trying to find a technology issue within the DoD will be easier with the Defense Technical Information Center than LOCC since it was designed just for this purpose.

As we build a classification scheme, we define topics and order them based on relative importance to our organization and their level of detail. Thus, Dogs and Cats are included in the Dewey Decimal System under Animal Husbandry because they are specific instances of the general field. But, how far do we go in listing animals? Should we scour the world

for every possibility and create a node for all animals? Do we include pets or do we create a separate heading for them, and if so, at what level of the taxonomy? These issues quickly arise while defining a taxonomy and lead to hair-splitting decisions about what nodes should be included and which are subordinate to others. As a consequence, taxonomies grow in size and complexity to the point that people cannot remember the classification scheme and cannot use it to mentally map their interests and needs. For example, the LOCC has greater than 6,000 nodes while SSIC has 2,500 nodes. Even specialized taxonomies that are small parts of general purpose taxonomies like the LOCC become large as they attempt to cover all the important topics in a field, such as with the physics taxonomy from the American Institute of Physics, a portion of which is shown in Figure 5.5-2. Note how the nodes get extremely detailed to the point that a non-physicist probably cannot understand what they mean, but for a physicist the nodes are still broad definitions since there are many sub-specialties under a topic as specific as III-V semiconductors (node 81.05.Ea).

80. INTERDISCIPLINARY PHYSICS AND RELATED AREAS OF SCIENCE AND TECHNOLOGY	
81. Materials science	
81.05.A	Specific materials: fabrication, treatment, testing and analysis
~~~~~	<i>Superconducting materials, see 74.70 and 74.72</i>
~~~~~	<i>Magnetic materials, see 75.50</i>
~~~~~	<i>Optical materials, see 42.70</i>
~~~~~	<i>Dielectric, piezoelectric, and ferroelectric materials, see 77.80</i>
~~~~~	<i>Colloids, gels, and emulsions, see 82.70.D, G, K respectively</i>
~~~~~	<i>Biological materials, see 87.14</i>
81.05.Bx	Metals, semimetals, and alloys
81.05.Cy	Elemental semiconductors
81.05.Dz	II-VI semiconductors
81.05.Ea	III-V semiconductors
81.05.Gc	Amorphous semiconductors
81.05.Hd	Other semiconductors
81.05.Je	Ceramics and refractories (including borides, carbides, hydrides, nitrides, oxides, and silicides)
81.05.Kf	Glasses (including metallic glasses)
81.05.Lg	Polymers and plastics, rubber, synthetic and natural fibers, organometallic and organic materials
81.05.Mh	Cermets, ceramic and refractory composites
81.05.Ni	Dispersion-, fiber-, and platelet-reinforced metal-based composites
81.05.Fj	Glass-based composites, vitroceraics
81.05.Qk	Reinforced polymers and polymer-based composites
81.05.Rm	Porous materials; granular materials

Figure 5.5-2—This portion of the physics taxonomy from the American Institute of Physics shows the extreme detail of the nodes.

This highlights the enormous complexity of creating an orderly method of classifying human knowledge and writings. We use the same words to convey different concepts depending upon the context of the discussion, what we expect other people to already know or not know, and how it relates to other activities and thoughts. If someone asks “How do we detect and track diesel submarines?” we can answer them by telling them what we know about state-of-the-art sonar transceivers and underwater acoustic wave signal processing, a listing of approved Navy anti-submarine warfare systems, a report on operational procedures, a statement of Navy organizations under Commander in Chief, U.S. Pacific Fleet (CINCPACFLT) involved in anti-submarine warfare, or even which acquisition programs develop and provide systems to the Fleet. In each case, the person asking the

question will be implicitly expecting their perspective to be the central theme since it is most important to them. If the actual classification framework, say an acquisition-centric one, doesn't match the user's perspective, they will have to hunt to find something they feel should be easy to find.

A taxonomy is a structured set of names and descriptions used to organize sources in a consistent way. A typical taxonomy uses a logical arrangement but doesn't account for users' particular decision-making and action-taking needs. A knowledge taxonomy focuses on enabling efficient and interoperable retrieval and sharing of knowledge, information, and data across the Enterprise by building in natural workflow and knowledge needs in an intuitive structure.

Extensive experience with Enterprise taxonomies in DoD, national intelligence services, corporate intranets, and the Internet has shown that Enterprise taxonomies must define which user perspective, or perspectives, will form the framework for the classification scheme (Sacco, 2000) (Glass, 1995). For example, an Enterprise taxonomy can be based on the core business areas, the organization hierarchy, primary product lines, or even an external scheme. Previous projects have shown that it is very difficult for a single classification scheme to capture the many concepts embodied in a document and the multiple perspectives needed to create an intuitive navigation scheme for all of a system's users.

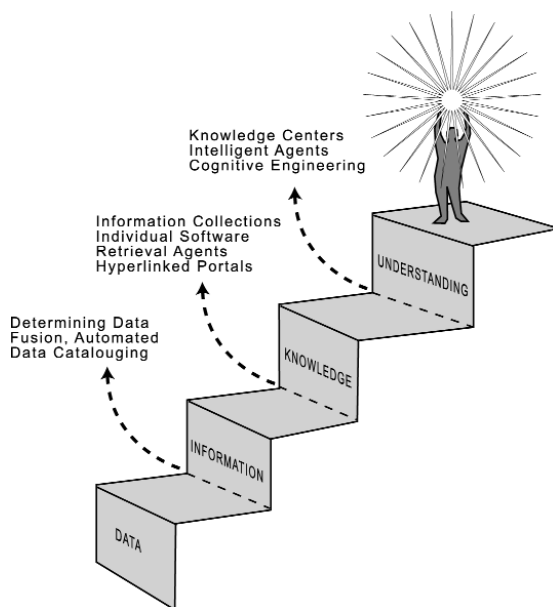


Figure 5.5-3—The Cognitive Staircase. Data is transformed into information, knowledge, and ultimately human understanding.

In order to construct a knowledge taxonomy, we must define what we mean by knowledge and how knowledge differs from information and data. Does a KM system provide automated access to all electronically available information across the Enterprise from a portal? Does it require full-time content creators and editors to produce summaries and analyses? Is a corporate personnel directory knowledge? The answer to all of these questions is: it depends! It depends on what the user needs to know at that moment and if that piece of information is all they need or only a small component of what they need. Figure 5.5-3 shows how information progressively moves from individual pieces of data that are devoid of context and relationships, up the cognitive staircase to information where pieces are grouped together, to knowledge

where disparate information sources are brought together and fused in a validated way, and finally into a human's cognitive processes as understanding. At each step, there are greater connections made among the variety of related items with authenticity and strength of relationships explicitly made. One type of knowledge taxonomy is the famous Bloom Taxonomy of Educational Objectives that outlines the major cognitive areas of thinking and analyzing (Bloom, et al, 1956). Bloom actually starts with knowledge and moves sequentially upward in cognitive skills (Rademacher, 1999) with the following major areas.

1. **Knowledge:** remembering previously learned material, recall facts or theories; bring to mind.
2. **Comprehension:** grasping the meaning of material; interpreting; predicting outcome and effects (estimating future trends).
3. **Application:** ability to use learned material in a new situation; apply rules, laws, methods, and theories.
4. **Analysis:** breaking down into parts; understanding, organization, clarifying, concluding.
5. **Synthesis:** ability to put parts together to form a new whole; unique communication; set of abstract relations.
6. **Evaluation:** ability to judge values for purpose; based on criteria; support judgment with reason (no guessing).

ONTOLOGIES

Ontologies are the conceptual framework that people are really trying to express in a classification scheme. When we talk about animal husbandry or anti-submarine warfare systems, we are actually considering all the context and relationships to other topics that we have as a general understanding of these topics in our society. When engineers talk about sonar systems, they do not have to keep asking about how this topic relates to sound waves in water since that is common knowledge in their field. Yet, this contextual link is critical to understand why acoustic transceivers are important and how they relate to submarine detection and tracking and other topics. In contrast, a non-engineer will likely not have this knowledge and therefore not understand why the others are discussing seemingly disparate topics like signal processing and sensor performance prediction algorithms. It is the group's general understanding of the concept of anti-submarine warfare systems that is the basis for classifying topics and determining which topics are more general and detailed to establish a hierarchy. These concepts inherently have connections to many other concepts with different strengths of relationships, as shown in Figure 5.5-4. Ontologies can be created for many applications and have many coordinating themes, such as business topics, technology functions, and tactical Military capabilities.

Ontology is the conceptual framework that people are really trying to express in a classification scheme. The ontology is translated into a hierarchy of descriptive categories that form the taxonomic schemes used to control the classification process.

The ontology is translated into a hierarchy of descriptive categories that form the taxonomic schemes used to control the classification process. Even with a detailed taxonomy, the classification scheme cannot convey the relative importance of the taxonomy nodes within the document nor the relationship among the nodes, which is exactly the contextual information needed to transform information into knowledge. A great deal of knowledge and context is lost as the concept, which often takes a group of people hours to discuss to refine its meaning, is distilled into one or a few words that act as its representation in the taxonomy. For example, the SSIC has a node titled Data/Information Archiving



under Operations and Readiness. As a user, this can also describe an information technology system function and therefore belongs under Information Technology or some other heading that starts with an information theme. Similarly, this topic can be about new data storage techniques, both hardware and software, and therefore belongs under a Research and Development heading. Each case is correct and useful but difficult to determine which is best without more knowledge on the context of how the topic is being used. One common method to alleviate some of this discrepancy is to use a thesaurus of terms to augment the terms used for the taxonomy nodes. This allows a wider set of words to form the basis of determining what is relevant to a particular node in the same way as we might use synonyms and antonyms to help someone understand a new word.

Users need a classification framework for the knowledge, information, and data that is consistent across the Enterprise but also allows individuals to intuitively navigate large volumes of resources. These seemingly conflicting objectives can be reconciled by constructing a knowledge taxonomy that blends the need for context and individuality with a consistent and structured framework.

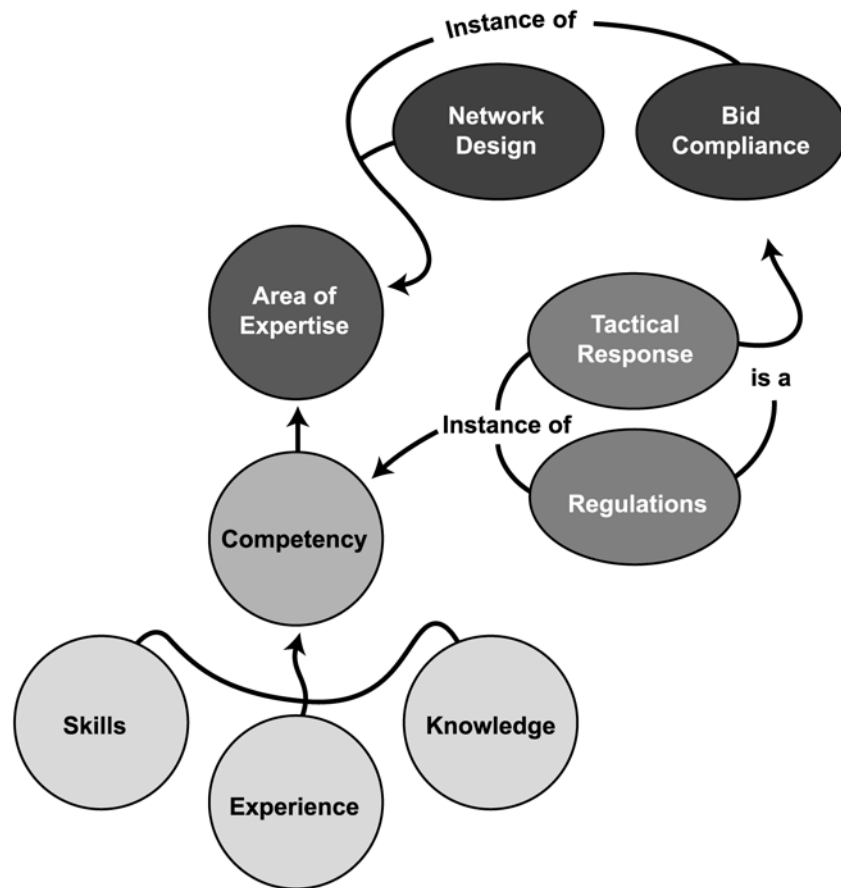


Figure 5.5-4—Concepts inherently have connections to many other concepts with different strengths of relationships.

THE ENTERPRISE KM TAXONOMY



In order to ensure that the lessons learned from many Enterprise scale projects are incorporated and current best practices are used, the Enterprise KM Taxonomy uses the following primary design principles:

- User effectiveness in retrieving, sharing, and storing data, information, and knowledge is the primary metric of success.
- Multiple perspectives of organizing schemes are needed to create intuitive navigational and classifying structures for the variety of user types.
- Local commands should be able to develop and use their own organizing scheme in addition to the schemes within the Enterprise KM Taxonomy.
- All of the domains, including locally developed sub-domains, must be completely cross-referenced to allow people to transparently access information across the Enterprise without having to struggle with different and non-interoperable schemes.

These principles lead to the following taxonomy architectural characteristics:

- Multiple domains and sub-domains.
- Significant overlap among domains is allowed to facilitate intuitive user navigation.
- Standard taxonomies are incorporated, such as Standard Subject Identification Code, Library of Congress Classification, and North American Industrial Classification System.
- New domains are created when user effectiveness could significantly decrease by coalescing partially similar schemes.
- Semantic flexibility is incorporated by including taxonomic thesauri and planning for an ontological framework.
- Policies will be issued to define standard taxonomic and extensible markup language (XML) methods for interoperability.

One key component of the approach is using a modular architecture of highly cross-referenced Enterprise scale and local workgroup level domains. However, this flexibility and user-centered architecture cannot be permitted to degenerate into a large number of disparate and non-interoperable classification schemes. All schemes must adhere to a set of adaptive but consistent standards and content management policies. The schemes can have substantial overlap in their domain entities if this can provide a significantly easier and more effective system. A mixture of customized and standard domains can be used to concurrently classify the data, information, and knowledge repositories, thereby allowing users to choose one or more of the domains depending on their particular perspectives and needs at that moment.

The Enterprise KM Taxonomy uses this mechanism to provide all users with an intuitive mapping of knowledge, information, and data resources. It has nine primary domains that include custom developed topics for the DON's functional areas, as well as standard taxonomies such as Standard Subject Identification Code, Defense Technical Information Center, Library of Congress Classification, and the new North American Industry Classification System which was jointly developed by the USA, Canada, and Mexico to facilitate North American commerce. These domains are all mapped to the full knowledge, information, and data resources across the Enterprise. To avoid users having to learn other taxonomy frameworks, they are completely cross-referenced in a central meta-data registry that acts like an exhaustive index of all categories and how they map across taxonomies. These domains are chosen to provide a variety of perspectives to the same information. This multifaceted classification is known to represent knowledge, information, and data content better than the typical single theme taxonomies like the Dewey Decimal System, Library of Congress Classification, and Standard Subject Identification Code (Taulbee, 1965). Indeed, a formal approach to multifaceted classification dates back to the 1920s when the Colon classification system was developed. This method breaks down the content into a set of terms with primary characteristics that can then be arranged in any hierarchical pattern that suits individual users (Ranganathan, 1957).

An Enterprise scale taxonomy should incorporate corporate and local workgroup level classification schemes to allow users to choose the most intuitive organizing framework for

their particular needs. Different schemes must be defined for various portions of the Enterprise. In order to avoid a chaotic system of disparate schemes, all scheme developers must adhere to a flexible but consistent set of standards and policies.

Initially, the Enterprise KM Taxonomy used the following set of primary domains:

- DON organization.
- Geography (standard country codes and DON locations).
- DON functional areas (22 sub-domains): Acquisition; Administration; Allies; Civilian Personnel; C3; Financial; Information Warfare; Intelligence and Cryptology; Logistics; Manpower; Medical; METOC; Modeling and Simulation; Naval Nuclear; Reserves; Readiness; Religion; Requirements, resources, assessments; Science and Technology; Test and evaluation; Training; Weapons.
- Library of Congress (government and general purpose standard).
- Defense Technical Information Center (DoD standard for technology systems).
- Universal Naval Task List.
- North American Industrial Classification System.

A KM taxonomy should use multiple primary domains to map all data, information, and knowledge repositories to allow users to choose the most intuitive domain or domains for their particular needs. Examples are business functional areas, organization, technology, and government standards. These domains can include customized schemes focused on the corporation's specific work environment and standardized schemes such as the Library of Congress. The taxonomy domains and the original twenty-two functional areas were reviewed by a working group comprised of major stakeholders according to the major design precepts listed earlier. Through this process, the working group learned that the original DON functional areas did not accurately reflect the primary task areas across the DON Enterprise. They determined that the entire functional area domain should be changed, and that the number of sub-domains limited to about ten to promote greater usability. However, the existing twenty-two functional areas are already being used in the DON and are possibly Chief of Naval Operations standard. Consequently, in keeping with the KM principle of focusing on user effectiveness, this domain was kept but renamed to allow users who need this thematic framework to have access to it. The new DON functional areas were defined through a usability sampling of stakeholders and became:

- Logistics
- Operations
- Installations and Facilities
- Administration
- People
- Acquisition
- Education and Training
- Science and Technology, Research and Development, Test and Evaluation (STRDTE)
- Medical
- Intelligence
- Finance

The Enterprise KM Taxonomy will be implemented on the federated architecture of application services and meta-data repositories and registries being developed by Task Force Web and NMCI. This architecture uses physical databases and information repositories linked to a virtual network. The Enterprise KM Taxonomy will be the classification framework unifying the meta-data within the federated architecture.

Ultimately, the Enterprise KM Taxonomy will be implemented in XML to be part of the Enterprise portal and application architecture of TFWeb and NMCI. This work is coordinated with the XML Working Group of the Data Management and Interoperability IPT as part of application integration planning. The central issue is the ability of the portal system to incorporate the functionality of meta-data and XML repositories and registries for information retrieval as well as eCommerce and data warehousing. The Enterprise KM Taxonomy will exist within an XML scheme that establishes the data structures for applications to use the predefined elements and attributes. Once a scheme is populated with actual data, it becomes an XML document and can be used for operations.

CONCLUDING THOUGHTS

The final interim version of the taxonomy is being distributed by DON CIO along with a policy statement for its use with information retrieval and KM systems throughout the DON. The next phase of this project is working with TFWeb and NMCI to build the Enterprise KM Taxonomy into XML meta-data scheme, namespace, repository, and registry to integrate with the Enterprise portal and its embedded search and classification engines. Performance measurements are now being collected on the combined taxonomy-portal system and used to analyze and modify both the taxonomy and the portal architecture and setup. In addition, the working group is starting to define the next set of policies and standards to incorporate greater contextual meaning through the use of an ontological framework in XML. This is the forefront of information and knowledge management systems and uses prototype ontology frameworks such as Ontology Interchange Language and Ontolingua.

Creating an intuitive yet consistent classification framework for all DON knowledge, information, and data allows us to finally corral our information systems and exploit their great potential to enable greater DON efficiency, effectiveness, and innovation. We cannot blindly pursue this path or we will fall prey to the same narrow focus that hampers so many of our IT systems, and which NMCI and TFWeb were specifically created to streamline. Only by continuously and vigilantly measuring and adapting our tools to user processes and needs can we ensure that we are truly achieving the goals of KM to quickly and precisely share and reuse knowledge throughout the DON Enterprise whenever and wherever it is needed.

5.6 Smart Card

Smart cards are the enabling technology required to support deployment of Public Key Infrastructure (PKI) in concert with Web enablement to power secure eBusiness within the DON. A key component of business process reengineering, smart card technology will greatly benefit Sailors and Marines.

—Rob Carey, eBusiness Team Leader

BACKGROUND

Smart cards are credit-card size, plastic cards that contain a microprocessor integrated circuit chip that stores and processes information. Smart cards comply with the standards set by the International Organization for Standardization (ISO), and may employ other technologies such as magnetic strips, bar codes, non-contact and radio frequency transmitters, biometric information, encryption and authentication information, and/or photo identification.

Smart card technology is used worldwide to enable electronic processes and transactions. For instance, in France over 100 million smart cards are used in pay telephones throughout the country. In Germany over 78 million smart cards were personalized and issued to German citizens as a health insurance card. In Hong Kong consumers are using Visa Cash cards as a replacement for currency.



The Department of the Navy (DON) has long been a Federal leader in smart card development. The Department first employed smart card technology for pilot projects in 1997. Over 500,000 DON personnel either possess or have used a Navy smart card. Sailors stationed in Naval Air Station (NAS) Pensacola and NAS Oceana use smart card technology to track their meal consumption at the base galley. From June 1998 through the end of 2001, each recruit entering the Naval Training Center in Great Lakes, IL received a card and used it for initial outfitting, immunization records, and food service. On ships, smart cards are used for quarterdeck access security, equipment accountability, and at-sea automatic teller machines.

The Common Access Card (CAC) is a smart card that is being issued throughout the Department of Defense (DoD). It is the new standard identification card for active duty members of the Uniformed Services, Selected Reserves, DoD Civilian employees, and eligible contractor personnel. It will be the principal card used to control physical access to controlled installations and areas, and control logical access to computer networks and systems.

The CAC will also be the Class 3 Public Key Infrastructure (PKI) token for all of DoD. This means that the CAC's integrated circuit chip will store the user's private key identity, e-mail, and encryption certificates. These certificates enable digital signatures, e-mail encryption, and access to secure Web servers and networks. This capability will secure information, reduce the dependency on paper and paper-based processes, and positively identify individuals in an electronic environment.

Smart cards combine multiple technologies on one plastic card—an embedded computer chip to store programs and data; a magnetic strip used for various applications, such as financial, debit, credit, and door key; and barcodes which can store more permanent information.

DESCRIPTION OF INITIATIVE

In November 1999, the Deputy Secretary of Defense signed a memorandum institutionalizing the use of smart card technology throughout DoD by directing that all DoD identification and access cards be replaced by the new CAC. This memorandum also designated the CAC to be the DoD Class 3 PKI token.

Congress has a keen interest in DoD smart card efforts. The National Defense Authorization Act for Fiscal Year 2000 directed the DON to work with the other Military Departments to develop plans for capitalizing on smart card technology. This act also chartered the Smart Card Senior Coordinating Group (SCSCG) and directed that the DON would chair this group. (The SCSCG is chaired by the DON Deputy Chief Information Officer (CIO) for eBusiness and Security) to ensure smart card interoperability throughout DoD and to maximize the potential of smart card technology.

The award of the Navy Marine Corps Intranet (NMCI) contract resulted in additional scheduling requirements for issuing the CAC to the 1.1 million DON Military, Civilians, and certain contractors. Because the CAC is the DoD PKI Class 3 token, it will be used for NMCI system log-on and is a crucial element of the Department's information assurance plan. Consequently, the CAC is planned to be issued to DON personnel before the NMCI seats are brought online and made operational.

Direction to pursue smart card technology extends from the highest levels. However, even without such direction, the DON CIO would lead the pursuit of smart card technology because it's the right thing to do. Smart cards streamline business processes; enable users to protect and share information more efficiently; reduce the number of cards users are required to carry; raise personnel quality of life; and increase mission readiness.

IMPLEMENTATION

The Department of the Navy Chief Information Officer is responsible for establishing strategic direction and Departmental policy concerning smart cards and the Common Access Card. The DON Smart Card Office (SCO) is leading both smart card implementation and Common Access Card issuance within the Department. In conjunction with these responsibilities, the SCO is also charged to help system developers utilize smart card technology as they strive to achieve the Department's vision of process improvements and eBusiness.

Successful employment of smart cards and the CAC requires significant changes to the Department's usual ways of doing business. As a result, smart card and CAC development

experienced a very unusual history of program management. It was also advantageous to execute a series of smart card pilots to, not only test the concepts, but also to prove the value of such systems. Successful CAC roll-out required very careful and flexible management strategies. Details of these experiences are discussed below.

Program Management

At the outset, the DON Smart Card Office (SCO) reported to the Director, Shore Installation Management on the Navy Staff. During this time, the SCO began many successful pilot programs using smart card technology. In April 1999, the DON CIO assumed responsibility for the office. As part of the Navy Secretariat, the CIO was in a more advantageous position to manage the program across the entire Department of the Navy (Navy and Marine Corps Commands). The CIO Office is also well suited to meet the smart card statutory requirements Congress placed on the DON.

One of the statutory requirements was to deploy smart cards to two carrier battlegroups (CVBGs) and two amphibious ready groups (ARGs) before June 30, 1999. The SCO led myriad efforts that accomplished this daunting challenge for the USS GEORGE WASHINGTON and USS KITTY HAWK CVBGs, the USS SAIPAN and USS BELEAU WOOD ARGs, and the 26th and 15th Marine Expeditionary Units. At the conclusion, over 30,000 cards were issued to crews and embarked Marines on 31 ships. To take advantage of this significant endeavor, smart card enabled systems for quarterdeck access security and equipment accountability were installed on those ships. Additionally, the existing at-sea automatic teller machines were modified to accept the new cards. The systems performed very well and they significantly improved what were paper intensive processes.

Through 2000, the Smart Card Office continued to support the smart card projects, wrote a smart card deployment strategy, and prepared for the Department wide issuance of Common Access Cards. In March 2001, that issuance began as the first of over one million CACs to be issued.



By Summer 2001, smart cards had proven their role as a significant enabler of process improvement, and CAC issuance was well underway. The time was right to shift smart cards to a more formal program management environment. It was also a good time to take advantage of programmatic synergies available at the DON Electronic Business (eBusiness) Operations Office. This office was chartered in September 2000 with two primary missions: (1) to be the DON's innovation center for eBusiness transformation and (2) to manage all DON card programs and selected electronic transaction systems.

Therefore, in October 2001 responsibility for the Smart Card Office shifted to the DON eBusiness Operations Office. The DON CIO retained responsibility for Departmental smart card policy, strategic direction, and oversight. This was not simply a shift in program management responsibility; the SCO physically moved to the eBusiness Operations Office at the Naval Supply Systems Command in Mechanicsburg, PA. The Department's continued efforts with smart card applications, CAC deployment and advances, and the other card systems will benefit from shared efforts and resources. Also,

since smart cards are a prime enabler of eBusiness, the Operations Office's eBusiness efforts will benefit by the close proximity of the DON's smart card knowledge base.

Smart Card Programs



The DON Smart Card Office supports pilot smart card applications across the Department of the Navy. These projects are valuable for several purposes.

First, they prove the value of smart cards as an enabler for improved processes. They also provide knowledge on how best to apply smart card technology. Furthermore, the commands that hosted the projects benefited from significantly more efficient processes. Finally, the project successes helped "sell" smart card use to the Department.

Smart card applications are currently in use at NAS Pensacola, NAS Oceana, Fleet Combat Training Center (FCTC) Atlantic Dam Neck, Marine Corps Air Station (MCAS) Kaneohe Bay, Naval Station (NAVSTA) Pearl Harbor, and numerous ships. In this context, "application" refers to redefined processes that integrate smart cards and for which software was explicitly designed.



Recruit Issuance



Food Service



Weapons Issue



Medical and Dental Applications



Figure 5.6-1—Smart Card Usage

To better demonstrate the broad applicability of smart card enabled processes, the pilot projects cover a wide range of functions. Further, they will be modified to operate with the Common Access Card prior to CAC deployment to these sites. The project applications include:

- Joint Food Service application streamlines galley operations.
- Joint Warrior Readiness maintains comprehensive data on an individual's readiness for deployment.

- Joint Manifest Tracking tracks personnel as they arrive at a location, or embark and debark on a mission.
- Joint Property Accountability application supports command tracking and asset visibility of selected equipment assigned to individuals.
- Smart cards on the USS GEORGE WASHINGTON Battle Group (12 ships, 15,000 smart cards) provided Quarterdeck Control, equipment accountability, and immunization records.

The pilot project instituted at Recruit Training Command (RTC) Great Lakes, in June 1998, is an excellent example of improvements smart card-enabled processes can return. RTC is the Navy's single entry point for all new recruits and trains about 50,000 men and women each year.

Five smart card applications were initiated at RTC. They were as follows:

- The Card Issuance application facilitated the issuance of cards to each recruit and populated them with demographic data such as name, social security number, and unit identification code.
- The Stored Value application was an electronic purse system that allowed recruits to purchase goods and services from the Navy Exchange. Prior to this system, the cash management function was handled through a paper-based chit scheme.
- The Smart Immune application automated the record keeping and tracking of immunization while the Smart Dental Information application documented baseline dental status and dental treatment needs.
- The Food Service application streamlined the student's daily entrance into the dining facility and significantly improved the management of that facility by increasing the accuracy of headcount data, eliminating reluctant data entry, and reducing fraud, waste, and abuse.

While conducting the pilot programs, the SCO made a significant decision regarding the future of smart card applications within the DON. The office shifted from a "data-centric" to a "Web-centric" design philosophy. With the former concept, the data necessary to use an application is resident on the smart card. On the other hand, Web-centric cards contain credentials that allow users to access applications and data through the World Wide Web. This design removes smart card memory capacity as a design constraint, avoids the loss of valuable data if cards are lost, and avoids erroneous data by taking advantage of single authoritative sources. The number of systems supporting improved DON processes is essentially unlimited.

Common Access Card (CAC)



CAC implementation is a continuation of the Department's use of smart card technology. It also provides a significant advancement in the Department's deployment of Public Key Infrastructure. The Smart Card Office recognized a synergistic opportunity provided by the increased storage capacity of the CAC's integrated circuit chip, the need for a hardware based PKI token for NMCI, and employment plans for PKI. This contributed to the CAC's selection as the Class 3 Public Key Infrastructure token for all of DoD. One of the benefits of this decision is the

elimination of a need for a separate, additional PKI issuance system. Resident on CACs, the level 3 token will be issued through the Defense Enrollment Eligibility Reporting System (DEERS) and the Real-time Automated Personnel Identification System (RAPIDS) infrastructure.

As noted above, the Deputy Secretary of Defense directed the Military Departments to implement the Common Access Card. Since Congress had previously designated the DON as the lead for smart card technology, the DON leads the way for CAC issuance.



In the best of circumstances, issuing a new identification card to over one million people is a complex and difficult project. To achieve this goal the Smart Card Office developed detailed and innovative program management, as well as an aggressive public awareness campaign. Perhaps even more importantly, the SCO managers were responsive to external factors and difficulties encountered during program execution. They quickly adjusted their carefully laid plans to meet the new challenges.

The SCO devised two CAC issuance plans; one for mass issuance and another for sustainment of cards already in the hands of DON personnel. For the former, the office manages a pool of 60 temporary DEERS RAPIDS workstations which provide the flexibility to produce large numbers of cards at selected NMCI sites. The office also contracted for four trailers that each contain six of these temporary workstations. Assuming an issuance time of 15 minutes per card, each trailer is expected to produce over 160 CACs daily. The trailers and other temporary workstations are moved between DON installations according to the CAC issuance schedule. Only with this temporary capability could a command issue CACs to its entire population in a reasonably short period of time.

Figure 5.6-2 shows one of four “CAC-mobiles” used to accomplish mass issuance of CAC to DON active duty uniformed personnel, Selected Reservists, DoD Civilian employees, and eligible contractor employees.

Of course, every command will require sustained CAC issuance as cards expire, cards are lost, new people report, Military personnel are promoted, etc. This is nothing new. The DEERS RAPIDS Integrated Workstations have long been used for ID card issuance to active-duty and retired Military personnel and their dependents. However, to issue CACs these workstations must be upgraded. Also, because the CAC customer base is significantly larger, additional DEERS RAPIDS installations are required. Thus, timely CAC implementation requires the SCO to coordinate closely with the Defense Manpower Data Center’s DEERS RAPIDS Integrated Workstation upgrade and new installation schedules.

Despite the many successes of smart card applications, the prospects of a new ID card were not initially applauded across the Department. The SCO anticipated that managing cultural change would likely be the most difficult challenge of CAC issuance. Therefore, the SCO wrote and executed a communications plan that detailed an ambitious awareness and education campaign. The objectives of this campaign include: achieve awareness throughout DON that a new identification card is forthcoming; explain the details of the card; and convey the improved quality of service that systems enabled by the new card will provide.



Figure 5.6-2—The CAC Mobile Issuance Trailer issues cards to DON active duty Uniformed Personnel, Selected Reservists, DoD Civilian employees, and eligible Contractor employees.

CAC issuance began in March 2001 and, despite careful planning and beta testing, encountered difficulties with the issuance system managed by the DoD. Further, there were isolated incidents of CACs not being recognized or accepted at Military installations, Navy Exchanges, and other facilities. Naturally, these problems exacerbated the problem of acceptance.

To correct the systemic problems, the SCO office worked diligently and expeditiously with the several DoD organizations that “own” portions of the system to overcome the technical difficulties. By applying the concepts of systems engineering, this team corrected the issues and the CAC issuance rate steadily increased.



Solving the problem of cultural change and CAC acceptance was more difficult. It required a management team open to the ideas of others and a willingness to modify carefully made plans. The DON CIO chartered a three-person panel of expert program managers to review the entire CAC program. Panel members without any previous exposure or connection to the CAC were explicitly selected. The CIO desired a “fresh slate” look at the program untainted by preconceived notions. In the end, every panel recommendation was accepted and enacted by the SCO. For example, the original plan mandated that service members surrender their traditional identification card when they received a CAC. The panel recommended that Military members retain both cards until the CACs are more widely accepted. The SCO requested permission from the Office of the Secretary of Defense (Personnel and Readiness) for U.S. service members to retain two cards for a period of six months. The request was granted and this change alleviated some anxiety from DON personnel and provided a safeguard for instances of CACs not being honored.

Also, despite having an excellent communications plan, the SCO readily changed it in order to meet the emerging issues. The public affairs emphasis was shifted to card recognition. Utilizing print, video and television media, the SCO worked diligently to introduce the CAC to the worldwide DON population.

Any successful project has a sound set of metrics. Good metrics are even more important for the Smart Card Office. Of course, they are used for program management. They are also needed to demonstrate to DON decision-makers that the program is under

control and that issuance should proceed within their areas of responsibility. The SCO selected a condensed and salient set of metrics that populate a single page, easily discernable CAC Weekly Performance Report. The metrics are: Sustainment Workstation Upgrade Plan; Actual vs. Projected CAC Issuance; Average CAC Issuance Time; Average Workstation Operational Time (station up time); Actual CAC Production Rate (cards/workstation); Average CAC Failure Rate; and Average CAC Encode Time.

THE FUTURE

New CAC-enabled smart card applications will be developed based on needs and results of business process reengineering. To ensure interoperability, data standards for future applications will also be prepared. Further, the Smart Card Program Manager will maintain liaison across the DON, with DoD leadership, and with the other services as all go forward in the development of new applications.

SUCCESS STORY

As noted above, CAC issuance began in March 2001. Initially, several technical issues hindered the process. These were rectified and in the fall, issuance began in earnest. A few months later, over 200,000 cards had been issued. Because the CAC contains digital certificates, its deployment also implements Class 3 DoD PKI within the Department. PKI enables digital identification, signature, and encryption capabilities to a broad range of applications at various levels of assurance. In September 2001, a CAC was used to sign and encrypt an e-mail from an NMCI seat at Naval Air Facility Washington.

In May 1999, the Smart Card Food Service application was implemented in three galleys at NAS Pensacola that serve about 10,000 meals each day. This system significantly reduces the time diners spend in the entry line and, at the same time, increases headcount data accuracy. Upon entry, diners insert their smart cards into card readers and their meal eligibility information is displayed on a touch screen. The cashier validates and admits the diner by touching a single button on the screen. This process takes just a few seconds. The application also streamlines back-office accounting, auditing, and report generation; eliminates redundant data entry; and obviates the need for a significant number of preprinted forms.

Since the Smart Card Food Service application was implemented, the customer load on the three galleys increased about 20 percent. Directly as a result of this application, the galleys now serve 2000 more meals per day with six less people on the management staff.

In the Fall of 2001, the Common Access Card became the first Java-based smart card to ever receive a FIPS-140-1 Level 2 Certification by the National Institute of Standards and Technology. Since then, the CAC program has gone on to win numerous awards as the most aggressive and secure smart card implementation in the Western Hemisphere. Smart Cards are truly becoming the "passport to the eWorld."

5.7 Records Management

The Department of the Navy has embarked on a journey to deploy the largest electronic records management system in the world.

—Charley Barth, Records and Document Management Team Leader

BACKGROUND

A central theme in both *Joint Vision 2010* and *Joint Vision 2020* is the concept of Information Superiority. These documents describe how Information Superiority transforms information from a supporting element of our defense posture to an actual weapon for our forces. As with any weapon, it provides both an offensive and defensive capability; just as important, it requires a defense against being used against us. Information has evolved from a rudimentary capability to a complex and advanced weapon; however, this evolution is not moving at a pace measured by decades but at a pace measured by months, if not days. As the Department of the Navy (DON) tries to achieve information superiority it will rely more and more on its corporate memory and its records management repositories.

The concepts of a record and records management have been a part of the world for centuries. From the very beginning humans have documented and saved information that has been important to them. Some examples of our nation's most famous records include the Declaration of Independence, Bill of Rights, Declarations of war, the Kennedy assassination files, and thousands of others. But besides these "historical records," the Federal Government's track record on accurately maintaining critical files (whether paper based or electronic) that could potentially affect many people across the nation, was mixed, at best. Many stories have been written about missing medical records, death records, chemical exposure records, especially within the Department of Defense (DoD). It was because of these elements of missing information that DoD threw its full weight behind the Electronic Records Management (ERM) concept.

Records management processes are used to achieve adequate and proper documentation of Federal policies and transactions and effective and economical management of agency and organizational operations. There are several Secretary of the Navy instructions, DoD standards and Federal codes that govern Records Management. However, ERM is a relatively new concept in the Federal Government. The proliferation of the computer and its associated software programs has led to a glut of electronic records that need to be preserved for our nation and its citizens. Also, the government is just beginning to realize the potential of mining these records to help with daily problem solving.

Records: include books, papers, maps, photographs, machine-readable materials, or other documentary material, regardless of physical form or characteristics. Records Management: means the planning, controlling, directing, organizing, training, promoting and other managerial activities involved with respect to records creation, records maintenance and use and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

The National Archives and Records Administration (NARA) is the Federal agency in charge of saving and providing access to all of the permanent records the United States Government saves. NARA has stipulated that electronic records may be printed out on paper and the paper copy can be saved as the “official record.” This policy (GRS 20) will surely change over the next couple of years. It will soon become mandatory to save electronic records in their native format (or a standard electronic format) for the life of that record. The government has only begun to address the issue of ERM and the long-term storage of permanent electronic records. E-mails, agency Web sites, word processing documents, spreadsheets and slide presentations are just a few examples of electronic records that might need to be kept permanently. As can be derived from this discussion, records in digital form potentially pose critical challenges for the DON and the rest of government.

Government agencies today have little control of their corporate information assets recorded in electronic form. This is creating increasing risk within the agencies because of the difficulty in capturing or recreating this critical information. All Federal agencies are required to maintain effective control and management of their records. But while records are often conceived in terms of textual documents, such as letters and reports, they can take any form (such as video, photographs, and voice discussions). The most effective solution in today’s digital environment is through the acquisition of an ERM package that is in compliance with Federal laws and regulations.

The DON Records Management office is located at the Washington Navy Yard. This office provides guidance and policy to DON records managers throughout the world and provides an invaluable link to NARA as well. According to Jim Jensen, Department of Navy Records Manager, most of the DON still produces paper records and records are saved as paper. However, there is an increasing amount of electronic records being created and saved throughout the Department.

The DoD has created a design standard for DoD agencies that want to start saving electronic records electronically. Each agency must use a DoD-approved Records Management Application (RMA) that meets the DoD 5015.2 design criteria. This standard has been around since 1997 and has gained widespread acceptance and support throughout the Federal Government. In fact, in November of 1998, NARA recognized and endorsed the DoD standard as conforming with the requirements of the Federal Records Act and the implementing records management regulations found in 36 Code of Federal Regulations 1220–1238.

DESCRIPTION OF THE INITIATIVE



Under the leadership of the DON CIO, the DON started to think “outside the box” and looked critically at how it did business. Part of this forward thinking led to the DON becoming the first executive agency to develop a plan where the Department would buy all of its information technology (IT) (desktops, networks, services, support, etc.) as a managed service under a performance contract. In October 2000, the DON awarded the Navy Marine Corps Intranet (NMCI) contract to Electronic Data Systems (EDS). NMCI became the first contract of its kind to deliver comprehensive, end-to-end information services through a common computing and communications environment. This environment will enhance system and software interoperability and in turn enhance information superiority capability for garrisoned and deployed forces as well as individual users. Under NMCI, EDS will own and maintain all required desktop and network hardware and software, and provide all required IT services, including ERM.

As the NMCI contract was being developed, the DON CIO, in concert with both the Navy and Marine Corps records managers, undertook the responsibility of inserting the requirement for an ERM capability within the solicitation. There were two requirements placed in the solicitation. The first was that the solution had to be DoD 5015.2 compliant. DoD 5015.2-STD defines the basic requirements based on operational, legislative and legal needs that must be met by RMA products that are acquired by the DoD and its components. The standard outlines a baseline set of requirements for automated record-keeping that must be met in order to satisfy 44 U.S.C. 2902, and guidance and implementing instructions promulgated by the NARA when record-keeping processes are automated through the use of RMA software.

The second requirement was that the solution had to integrate with the Secretary of the Navy Instruction (SECNAVINST) 5210.11D (Standard Subject Identification Codes (SSIC)) and SECNAVINST 5212.5D (Disposition Manual). The SSIC manual provides the numbering taxonomy that the DON uses to save and retain its records. The Disposition Manual gives a detailed description of each SSIC number by defining the records and listing how long to retain the record. The Disposition Manual addresses electronic records in the DON as follows:

The disposition guidance in this chapter applies to electronic mail and word processing system copies of records covered in this chapter unless otherwise specified herein.

(Note: If a system used to generate electronic mail, word processing and other office automation based records does not have record-keeping functionality, the official record-keeping copy must be copied to a record-keeping system where it will be maintained for the period stated in this chapter. A record-keeping system is a manual or automated system which has record-keeping functionality, i.e., the ability to collect, organize, categorize, retrieve, preserve, and provide for records disposition. DoD 5015.2-STD, Design Criteria Standard for Electronic Records Management Software Applications refers.)

- a. *Copies that have no further administrative value after the record-keeping copy is made. Includes copies maintained by individuals in personal files, personal*

electronic mail directories, or other personal directories on hard disk or network drives, and copies on shared network drives that are used only to produce the record-keeping copy.

Destroy/delete within 180 days after the record-keeping copy has been produced.

- b. Copies used for dissemination, revision, or updating that are maintained in addition to the record-keeping copy. Destroy/delete when dissemination, revision, or updating is completed.*

Selection of a DON records management software package will be part of a standard suite of applications for use throughout the Department. Providing tools that enable employees to quickly and easily create, store, locate, access, and retrieve documents most certainly will have a positive impact on productivity and information superiority.

Further information regarding the DoD 5015.2 standard is available on the Internet at <http://jitic.fhu.disa.mil/recmgt/>. The Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC) Web site contains information regarding the RMA compliance test and evaluation (CTE) process and procedures that application vendors must complete before their software solutions can be implemented by DoD agencies. This site also includes information about RMA products that have been tested and certified as compliant with the standard. NARA has endorsed this standard for Federal use and has endorsed the certification process that JITC goes through to approve vendors. To date, there are over 25 solutions that have been certified.

WHY NOW?

The Electronic Records Management Application (ERMA) requirement was placed into the NMCI solicitation based on recent IT guidance. The Clinger-Cohen Act clearly states that the CIO has authority, responsibility, and accountability for the agency's information resources management activities, and providing for greater coordination among the agency's information. The Clinger-Cohen Act requires agencies to consider the potential to share costs and benefits across offices and applications when designing their information systems.

Office of Management and Budget (OMB) circular A-130 says...“Systematic attention to the management of government records is an essential component of sound public resources management which ensures public accountability. Together with records preservation, it protects the government's historical record and guards the legal and financial rights of the government and the public.” Also, A-130 says to “Incorporate records management and archival functions into the design, development, and implementation of information systems;” A-130 explains how agencies must implement Records Management. According to A-130, agencies will:

- Ensure that records management programs provide adequate and proper documentation of agency activities.
- Ensure the ability to access records regardless of form or medium.
- In a timely fashion, establish, and obtain the approval of the Archivist of the

- United States for retention schedules for Federal records.
- Provide training and guidance as appropriate to all agency officials and employees and contractors regarding their Federal records management responsibilities.

However, without the appropriate mechanisms or safeguards in place to ensure the authenticity and reliability of those documents that must be set-aside as records, corporate vulnerability during litigation, preservation and discovery, will inevitably be increased.

A corporate records management (records retention) program that is not applied consistently to all corporate information assets, regardless of medium of storage (technology), increases litigation risk, discovery, preservation, and production costs. This includes e-mail, electronic data sets, and other digital information, particularly those data that reside on desktop computers.

If your requirement is for an electronic records management system (ERMS), you should keep in mind that whatever records management application software you deploy must satisfy two overarching criteria:

- It must be capable of managing all organizational records regardless of storage media or other characteristics.
- It must implement records management procedures to ensure the capture and preservation of authentic and reliable records (as defined earlier).

IMPLEMENTATION

When making the decision to automate company records management practices, you will want to ensure the tools you deploy are capable of accomplishing your organization's records management objectives. If you can answer "yes" to the general requirements questions below, then the chances are good that your needs will be best satisfied by a records management system rather than a document management system.

Managing Organizational Records. Does the "system" (software) manage organizational records regardless of the media?

Implementing Records Management Procedures. Does the "system" (software) include automated records management procedures to help capture and preserve records and ensure their authenticity and reliability?

Maintaining Record Integrity. Does the "system" (software) maintain electronic records in a manner that will prevent alteration and safeguard against their premature destruction?

Regardless of DON's decision to automate the records management processes, or continue to maintain existing (manual) processes, there are several questions that records managers can ask themselves to help them gauge the extent to which their organizations could face litigation risks that may be associated with corporate records management practices (or the lack of same). Ask whether:

- Corporate records are managed consistently, regardless of the media on which they are stored (paper, tape, hard drive, diskettes, etc.).

- Policies, procedures and audit mechanisms are in place to ensure all employees capture and preserve records in a manner that will ensure their authenticity and reliability.
- There are policies in place, that employees are familiar with, regarding the creation, use, and preservation of corporate information (on office desktop computers, as well as data that is taken home and manipulated on employee-owned computers).
- Mechanisms have been instituted to prevent unauthorized alteration of electronic records and safeguard them against premature destruction.
- A backup strategy has been implemented and is consistently applied, that will ensure electronic records are properly preserved, reliable, authentic, and accessible.

In spite of DON's ability to have an ERM system rollout as part of the NMCI software load, there are many potential barriers to implementing ERM. Senior leaders across the Department must understand the potentials of the capability that is being deployed, and must be on board with the concept and the rationale of why it is installed on everyone's desktop. If senior management does not support the effort, it will be hard to expect our information producers to use it.

CONCLUDING THOUGHTS

These are exciting times for the Department. DON is the first agency to implement an Enterprise-wide electronic records management in the Federal Government. There has already been a series of requests for providing additional functionality within the ERM system that was chosen. Many agencies across the DON are looking for tools that perform document management, correspondence management, workflow, and knowledge management on top of records management. A consistently applied and effective corporate records management program, including those that have been automated, will facilitate the location and production of records subject to discovery in a more timely and cost effective manner. While success will be measured and judged some time in the future, one thing is known. At 411,000 seats on NMCI, the DON will become the largest electronic records management customer in the world.

CHAPTER 6

Focus On People

- 6.1 *IM/IT Workforce Competency Management*
- 6.2 *Integrative Competencies*
- 6.3 *Information Literacy*
- 6.4 *Organizational eLearning*
- 6.5 *Communities of Practice*
- 6.6 *Section 508*

INTRODUCTION

The current information technology (IT) revolution has few equals in any other period in history. Over the past decade, a peaceful revolution driven by the explosion in IT has occurred. IT provides users greater computing power in smaller packages at lower costs, and with that computing power comes an enormous capacity for change, driving process reengineering, new ways of doing business, and streamlining. The significant transformation in the Department of the Navy (DON) capitalizes on the awesome potential of advanced IT. Built on Network Centric Operations, the capstone concept for bringing networked organizations and technologies to bear in future battlespaces, the Department has developed insights into Knowledge Superiority, providing power through people—what they know, how they bring their knowledge together, and how they translate that knowledge into action.

INSIGHT

We live in a mental world where the potential of technology is both exciting and unlimited. It's so easy to get caught up in that excitement, and forget that the performance advantage comes from how technology is used. The real reward comes when people embrace these new tools to create, act upon, and share their ideas. In the end, the success of IT is dependent on people learning and growing.

Competencies are the knowledge, skills, abilities, and behaviors needed by individuals to achieve the mission of the Department. They empower decision-makers at all levels of the chain of command to make decisions and take the actions needed to do their jobs, i.e., providing the freedom and flexibility critical for success. The process of competency management entails figuring out exactly what those skills look like for the future, and developing a strategic approach to ensure those competencies are available when they are needed. In a dynamic environment with changing targets, this can only be successfully achieved through the use of Enterprise-wide teams that bring together the best expertise and thinking of the Department.

The journey to understand the competencies needed by the future DON workforce includes many experiences along the way. First, the Department needed to identify the type of work that needed to be performed by government, and the type of work that could be performed by contractor personnel. The DON Chief Information Officer (CIO) categorized work and determined that work which is inherently governmental affects strategic and tactical decisions about the DON workforce. The resulting Inherently Government Guidance helped ensure DON would retain the critical leadership and oversight capabilities it needed, and release to private industry the workload that would fiscally benefit from economies of scale, thereby creating the advantages of increased funds available for refining skills of DON personnel.

Development of a DON Information Management/Information Technology (IM/IT) Workforce Strategic Plan provides a roadmap for the future workforce, and a shared vision for all parts of the DON organization. It improves the way DON administers the key process of workforce management—setting requirements, recruitment and hiring, training and education, job placement, retention, and leadership. A Civilian Career Path Guide offers employees and supervisors the opportunity to build a career progression plan for gaining excellence in a current job, or qualifying for a future job. The five career areas developed for the IM, IT, and knowledge management (KM) workforce include Information Management, Knowledge Management, Computer and Information Systems Engineering, Information Assurance, and Telecommunications. A Career Planning Tool provides a resource for virtually managing an individual's career.

There are different types of competencies that form the foundation of high performing organizations. Integrative competencies, a set of fundamental skills that enhance working in a virtual environment, enrich an individual's cognitive abilities and enable connectivity and integration of other competencies, leading to improved understanding, performance, and decisions. Integrative competencies addressed by the CIO organization include Information Literacy, Knowing, Knowledge Management, Systems Thinking and Organizational Learning.

Today's workplace demands a new kind of worker. In our global world, data is dispatched in picoseconds and gigabits and this deluge of information must be sorted, evaluated, and applied. Information Literacy is a set of information and knowledge age skills that enable individuals to recognize what information is needed, when it is needed, and methods for location, evaluation, use, and effective communication. It is people knowing how to use what the Department—and the world—is creating.

In today's world, learning is taking more and more advantage of information technology. Challenged by the rapidly changing environment in which they must function, and by the emerging associated competency requirements, people must keep pace with new challenges and situations. To do this they must continuously learn new approaches. Information technology facilitates the opportunity to do just that. As people learn and share what they learn with others, the organization learns. This is the focus of *Learning in a Virtual World*, a CD toolkit developed by the Department that provides a wealth of information and knowledge on the new eLearning field and information on Defense learning resources.

Emerging across the Department, Communities of Practice are facilitating individual and organizational learning. Communities of Practice are one of the first new organizational forums of the millennium. Built on the tradition of professionals joining together to share skills and resources, communities are all about people, offering a rich forum for knowledge sharing, relationship building, and creative thinking. In both their formal and informal forms, they are adding value to the bottom line of the individual and the organization.

Finally, important changes are being undertaken to ensure employees and public customers with disabilities have access to the information they need. Section 508 of the Rehabilitation Act directs all Federal agencies to ensure accessibility of hardware, software, Internet and intranet systems, Web sites and e-mail, video and multimedia, information and transactions machines, and equipment used for transmitting, receiving, using, or storing information.

As we build our knowledge systems, develop our Enterprise portal, and connect across the Navy Marine Corps Intranet (NMCI), the Department must ensure that the information needed by decision-makers can be accessed, understood, and used by all decision-makers. In the end, it's all about people.

6.1 IM/IT Workforce Competency Management

People are important, and we must invest in them. Our IM/IT Workforce Competency Management program will help us identify specific ways to hire and develop the people who have the knowledge, skills, abilities, and behaviors needed to meet the technology, information, and knowledge requirements of the Department of the Navy, now and in the future.

—Sandra J. Smith, IM/IT Workforce Competency Management Team Leader

BACKGROUND

The challenges of a high technology workplace are significant. Information technology (IT) has the power to transform the functions of government, increasing the demand and accountability for performance excellence. To realize this goal, the Department of the Navy (DON) must be able to attract and retain the very best workforce to develop, implement, and manage a wide variety of information technology systems.



The Federal Government is increasingly aware of the value of people to achieving an agency's mission. The Comptroller General of the United States, David Walker, has stated that people need to be viewed as assets in which to invest, vice costs to be cut. Section 5125 of the Clinger-Cohen Act (CCA) of 1996 specifies a Chief Information Officer's (CIO's) responsibility for workforce capabilities. Specifically, it requires CIOs to provide guidance for developing plans for hiring, training, and professional development to meet workforce needs for information technology and information management (IM) skills. This affects the entire workforce, not merely the professional IM/IT "core." Section 5125 also charges the CIO with providing advice and assistance to the agency head in the management of information. Related legislation, the Paperwork Reduction Act of 1995, tasks CIOs with assisting the agency head with management of information to promote decision-making. This supports the inclusion of knowledge management (KM) in the DON CIO charter. The DON CIO also guides Enterprise-wide achievement of the DON IM/IT strategic goal to refine core capabilities and shape the workforce that is—and will be—responsible for the management of technology, information, and knowledge.

APPROACH

In 1999 the DON CIO invested in the planning for the Department's human capital by creating a dedicated team devoted to IM/IT Workforce Competency Management (competencies are defined as knowledge, skills, abilities, and behaviors). A government and contractor team began the task of creating an Enterprise approach to the IM/IT workforce. This approach focused on a strategy for leveraging human capital by considering four key issues: (1) ensuring we recruit, retain, and train the IM/IT/KM workforce needed to fulfill core capabilities, (2) establishing IM/IT/KM competency guidelines for the non-

IM/IT/KM workforce, (3) developing IM cognitive skills through integrative competencies, and (4) ensuring the IT infrastructure will support eLearning, document best practices, and expand the use of eLearning technologies.

Capitalizing on CIO direction, feedback from claimant-level CIO staff, and building on best practices and initiatives from other Federal agencies, the IM/IT Workforce Competency Management Team developed an overall approach to understanding workforce issues and translating the concerns into CIO action. This data gathering surfaced needs for guidance that touched both the Enterprise and the employee. The result was a multifaceted approach to the workforce that responded to the issue of a widely recognized, national-level crisis in recruiting and retaining adequate IM/IT talent.



The DON CIO chartered a cross functional/cross organizational Integrated Process Team (IPT) to examine the issues and identify policies and practices to support the DON. Membership was deliberately broad—spanning the spectrum of Marine Corps, Navy claimants, and SECNAV organizations that were stakeholders either by virtue of their sizeable IM/IT/KM workforce, or their responsibilities for human resource (HR) policy and procedures. The IPT sought input from a myriad of sources across the public and private sector, and ended up designing a process based on the workforce-planning model developed in 1999 by the Office of Personnel Management (OPM). The process starts with setting strategic direction, identifies the supply and demand of workforce requirements, develops a plan to accomplish specific goals, and ends with establishing a systematic approach for monitoring and evaluation.

Based on the model, the IPT identified Enterprise-wide workforce requirements for the FY2000–2005 timeframe. Their actions included:

- Creating the DON IM/IT Workforce Strategic Plan.
- Refining DON CIO guidance on inherently governmental and non-inherently governmental functions.
- Creating the DON Civilian Career Path Guide for the Management of Technology, Information and Knowledge.
- Developing an automated, interactive Career Planning Tool.
- Developing guidance for Continuous Learning, to help ensure the workforce stays current with rapidly evolving changes in IM, IT, and KM.
- Performing strategic workforce planning for the Military and Civilian workforces, looking ahead to FY2005 to estimate the demand for workers and the expected supply available to fill those requirements.

IM/IT Workforce Strategic Plan



The DON IM/IT Workforce Strategic Plan presents the roadmap for a systematic approach to IM/IT workforce planning in the DON. It identifies goals and objectives to ensure we have “the right people, with the right skills, in the right jobs, at the right times.” It was created over a one-year period, and during this time the shared vision enabled initial implementation of the Plan before it became an official document. The document was officially endorsed by

the critical stakeholders in HR and in IM/IT—those working for the Secretary of the Navy, the Chief of Naval Operations, and the Commandant of the Marine Corps. This senior leadership in both the IT and HR communities demonstrated the partnership needed to achieve the goals and helped to reinforce buy-in for the recommended changes. The Plan became not so much a plan to shape a workforce directly, but to improve the way we administer the key processes of workforce management—setting requirements, recruitment and hiring, training and education, job placement, retention, and leadership. This Plan is unique, and offers a model capable of replication across Federal Government to assist in leveraging human capital.

Inherently Governmental IM/IT Functions



This guidance defines IM/IT functions and the type of work performed by government and contractor personnel. By categorizing work, we can make strategic and tactical decisions about the workforce. The resulting “Inherently Governmental Guidance” was used by CIOs and other affected organizations throughout the DON as the Enterprise took steps to comply with the Federal Activities Inventory Reform Act of 1998 (FAIR Act) by annually marking jobs that would be considered for outsourcing, and by planning commercial activities studies to determine if the functions those jobs represented should be outsourced. The guidance helped to ensure the DON would retain the critical leadership and oversight capabilities it needed, and release to private industry the workload that would fiscally benefit from economies of scale and the advantages of increased funds available for refining skills.

Civilian Career Path Guide (CPG)



Focusing on the individual, the IPT sponsored the development of the DON Civilian Career Path Guide (CPG) for the Management of Technology, Information and Knowledge, a two-volume guide published by the DON CIO in March 2001. Overall, the CPG describes a career development process (see Figure 6.1-1) used by an employee and his supervisor or mentor to build a Career Progression Plan for gaining excellence in a current job or qualifying for a future job. The CPG defines five career areas for the IM/IT/KM workforce: Information Management, Knowledge Management, Computer and Information Systems Engineering, Information Assurance, and Telecommunications. The CPG documents an extremely broad spectrum of work—from research and development, to acquisition, to operations and maintenance—and focuses on the inherently governmental functions necessary to lead and oversee this work. It also includes original thinking in knowledge management, defining the job roles of KM practitioners and listing the competencies that drive excellence. In a holistic approach to human capital, the Guide cites “Career Foundational” (or professional) competencies that complement technical (or functional) expertise in the top-quality DON employee. These competencies are based on those promoted under the DON Civilian Leadership Development Program.

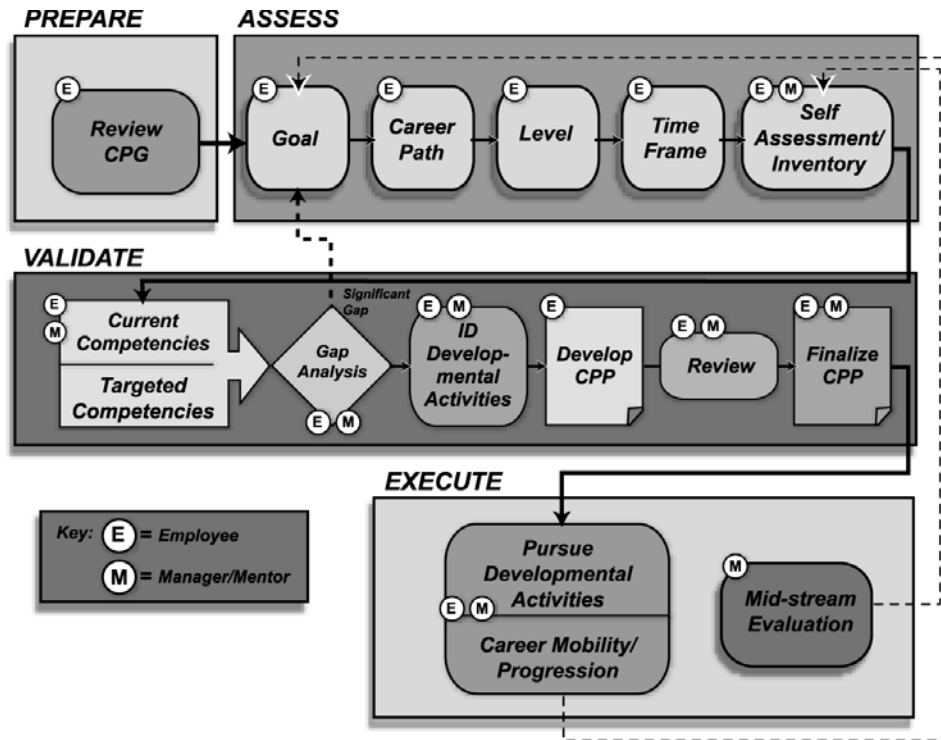


Figure 6.1-1—DON IM/IT/KM Career Development Process

Career Planning Tool (CPT)



The Career Planning Tool was developed to provide a resource to assist DON Civilian IM/IT employees in managing their careers. The CPT is an interactive database application based on the Career Path Guide for the Management of Technology, Information and Knowledge. The CPT enables individuals to assess their own proficiency in functional and professional competencies. The functional competencies are related to specific job functions and are grouped into the five broad career areas. Also included are professional competencies that apply to all employees—comprised of things like teamwork, leadership, strategic vision, and other necessary professional competencies. The tool allows users to determine where gaps exist in terms of competency proficiency, and enables them to design a tailored development strategy to help achieve proficiency in those competencies. With this information, the CPT can be used to develop a Career Progression Plan that contains four parts: (1) Career Development Data, (2) Needs Analysis, (3) Development Strategy, and (4) Development History. The tool, based on the user's self-assessment of competencies, automatically generates most of the Career Progression Plan, which can be printed out and shared with or approved by the individual's supervisor or mentor. DON CIO continues to improve the tool with periodic upgrades. The next revision will expand the five functional areas for the new occupational series Information Technology Management, GS-2210 that includes 10 parenthetical titles used in addition to the basic title to identify specialty areas and selective qualifications: Policy and Planning, Security, Systems Analysis, Applications Software, Operating Systems,

Network Services, Data Management, Internet, Systems Administration, and Customer Support. While these competencies are already included in the tool, they will be provided with a more explicit view.

Continuous Learning Guidance



DON leadership appreciates the concept of the “learning organization.” This concept was fundamental to the thinking that drove the design of the DON CIO organization. For the IM/IT/KM workforce, methodologies and tools change continuously. Workforce members face a continuous challenge to remain current in their disciplines, retaining the ability to identify, acquire, and employ the IM/IT/KM capabilities necessary for mission success. People must become lifelong learners in order to maintain their currency. To carry the learning theme into the workforce, Continuous Learning Guidance was published in July 2000, recommending 80 hours of professional update for all Civilian and Military IM/IT core workforce professionals each year that would augment the competencies established in their career fields and required for specific assignments. Venues were not restricted to those employing traditional training and education modalities, but expanded to encompass conferences, mentoring situations, rotational or on the job skill development assignments, and other learning opportunities.

WORKFORCE PLANNING

DON needs to ensure that appropriate action is taken by doing the right planning to recruit, develop, and retain a highly talented workforce. The government is facing a mass exodus of highly talented individuals through retirement, competition with private sector, and lack of interest in working for government. We also see changes in attitudes and expectations as new generations of workers integrate into our workforce. As a result of these factors, there is an increased interest in workforce planning. Workforce planning is not a new topic, but how the DON is approaching it is new. We are not focusing on just how much money and how many people—but rather ensuring we take a strategic view of the workforce by focusing on the needs of the Department, what competencies are required, and changes in functions resulting from changing missions, processes, and environmental factors. To this end, we are developing policies and procedures to support our workforce and looking at content and composition of the workforce as it relates to mission.

All DON CIO efforts in IM/IT community planning have taken into consideration the major studies that were available as the work went forward. This includes the Naval Personnel Task Force documents, as well as the National Academy of Public Administration study on the Civilian workforce (Civilian Workforce 2020: Strategies for Modernizing Human Resources Management in the Department of the Navy). As we move into the 21st Century, the DON vision—as described in The Maritime Concept and the Navy’s Strategic Planning Guidance—is to ensure that future Naval forces can exploit new opportunities and capabilities to project power and influence anywhere in the world in the Information Age. This extraordinary ability to exploit the power of information and knowledge focuses unprecedented interest on the IM/IT workforce. It is essential that the DON ensures it has the policies, practices, and resources to develop the versatile, motivated workforce needed to leverage the IM/IT environment.

Building on the DON IM/IT Workforce Strategic Plan, the degree to which the DON could anticipate a capability gap in FY2005 was evaluated—a difference between the demand for IM/IT/KM talent and the projected supply. Mechanisms for overseeing the Military workforce differed significantly from those available to administer the Civilian workforce. Thus, each required tailoring.

Gap Analyses and “Call to Action” strategies teams were sponsored to specifically examine the current and future workforce, the current and future IM/IT workload—and the gap that is projected for the future—by the year 2005—between the workforce and the workload. These teams also looked at competencies and the gap that is projected. By examining the gaps, we will be able to identify strategies that could be implemented now, that will help shape the workforce to meet future requirements. These studies were proof of concepts that demonstrated the power of workforce planning. The aim was to use this process as a tool to aid in making future decisions.

The DON IM/IT Civilian Workforce gap analysis used a high-level work breakdown structure to estimate workforce and workload, both current and future. A secondary analysis focused on the critical competencies available now, compared with projected needs for these competencies. Finally, a “call to action” strategy was created, identifying the primary actions recommended for closing the gap.

The DON IM/IT Military Working Group was chartered to conduct a workforce analysis, using a team of IM/IT and human resource experts from across the DON and drawing on existing manpower sources. They focused on “core” IM/IT personnel of the Navy and Marine Corps—officer and enlisted personnel, regular and reserve component—with the following objectives:

- Determine the current and future level of IM/IT work (demand).
- Identify the current and future personnel that will perform the work (supply).
- Analyze the gap between workload and workforce and the factors contributing to the gap.
- Assess the competencies—knowledge, skills, abilities, and behaviors—needed by the workforce to do the work of the organization.

The Military Working Group also identified strategies and associated initiatives to help the DON mitigate the gaps identified, and attract, retain, and train a quality Military IM/IT workforce.

The Military Workforce gap analysis benefited from rich sources of electronic information. The challenge lay in integrating them to form the needed picture of today’s and tomorrow’s situations. The team similarly identified gaps—but more along the lines of needs to change procedures for funding, defining requirements, recruiting, training/education, and placing, organizing and retaining these key Military assets. They also constructed “call to action” strategies for mitigating the gap.

INTEGRATIVE COMPETENCIES

The DON CIO launched an aggressive program to develop learning materials in support of integrative competencies, a set of fundamental skills that enhance working in a virtual environment. Recognizing that there are different types of competencies that form the foundation of high performing organizations, integrative competencies were viewed as a means to enhance other competencies, whether functional or professional. Integrative competencies have a multiplier affect through their capacity to enrich an individual's cognitive abilities and enable connectivity and integration of other competencies, leading to improved understanding, performance, and decisions. Integrative competencies can address functional "white space" and can improve an individual's ability to learn. These competencies include Information Literacy, Knowing, Knowledge Management, Systems Thinking, and Organizational Learning. The DON IM/IT Workforce IPT focused on fostering specific integrative competencies for the entire DON workforce—not merely the core IM/IT/KM professionals. Building on prior work of the DON Acquisition Reform Office, the DON CIO furthered a program in critical thinking, promoting the use of Systems Thinking to lessen the complexity of decision-making. The DON CIO sponsored several face-to-face classroom sessions, then developed computer-based training with examples of DON applications, and made that training available to all DON members. Related to this discipline is Information Literacy, another competency that helps individuals integrate information and apply it to decision-making. To fill this gap, the *Information Literacy Toolkit* was developed and has been made available to all personnel as a resource through either CD or the Web. Continuing to expand learning resources for the Department, the *Learning in a Virtual World* CD was developed that focuses on operationalizing eLearning and providing people with a single source to "learn about learning" and information on learning resources. For additional information, refer to the sections in this chapter on Integrative Competencies, Information Literacy, and Organization eLearning.



DON CIO has responsibility for taking a special look at a specific community—the DON Information Management, Information Technology and Knowledge Management workforce. With our current emphasis on technology, this community attracts a high interest, primarily due to increasing overall dependence on IT to getting jobs done. To provide a resource for the community members, DON CIO developed the *WORKFORCE* CD. The CD provides a single source for guidance and tools for the IM/IT community, including the DON IM/IT Workforce Strategic Plan, Guidance on Inherently Governmental IM/IT Functions, Continuous Learning Guidance, the Civilian and Military Gap Analyses, Career Path Guide, and the Career Planning Tool. All these tools are also available at www.don-imit.navy.mil.

THE FUTURE

The IM/IT Workforce Competency Management program will continue to shape the future IM/IT/KM workforce, focusing on the requirements generated through a changing technology base. Competencies will change with the emergence of new technology and

roles. Additionally, the outsourcing of IT support through the Navy Marine Corps Intranet, changes the demand for certain work. These factors affect the kind of people we need. We now see more emphasis on knowledge workers—people with the ability to create, apply, and use information. As the DON inserts new technology and develops new organizational structures, demand will drive additional requirements for specific competencies. For example, growth of knowledge management and eGovernment, and the increased emphasis on Information Assurance will affect the level and type of required workforce competencies. The roadmap for change will continue to be through the implementation of the goals and objectives of the DON IM/IT Workforce Strategic Plan and sponsorship of innovative pilot projects.

A revision of the DON IM/IT/KM Civilian Career Path Guide will improve the Career Planning Tool by incorporating the new job family standard for administrative information technology work. OPM designed the new occupational group, the Information Technology (IT) Group, GS-2200, to cover all positions previously assigned to the Computer Specialist Series, GS-0334, as well as positions classified in other series (e.g., the Telecommunications Series, GS-0391, and the Miscellaneous Administration and Program Series, GS-0301) where IT knowledge is paramount. The initial occupation in this job family is Information Technology Management, GS-2210, which will be folded into the career areas of the CPT and made available for use across the Federal Government.

The workforce “call to action” strategies will be executed to prepare the DON for a sustainable competitive advantage in IM, IT, and KM. The IM/IT Workforce Competency Management Team will continue to lead the formulation of policy and guidance for workforce planning, recruiting, assigning, and retaining the core IM/IT/KM capabilities needed to achieve Knowledge Superiority.

The DON IM/IT Military Working Group developed strategies and recommendations to mitigate the Military IM/IT workforce and competency gaps. The cornerstone strategies form the basis of recommendations to take forward to an implementation working group. The DON CIO is committed to building a cross-functional team and collaboratively working to develop strategic actions that will result in improved manpower and personnel policies and procedures. Numerous efforts focus on improving manpower and personnel management across the Navy and Marine Corps. These groups are sharing information, concepts and strategies, so that all efforts are benefiting from the others’ experience and expertise. This dialogue is key to facilitating Enterprise-wide changes.

To attract and retain a talented workforce in the future, DON CIO is promoting and developing partnerships to integrate the recommendations of the National Academy of Public Administration in their recent report, “The Transforming Power of Information Technology—Making the Federal Government an Employer of Choice for IT Employees” released August 2001 (see Figure 6.1-2). One finding of the report addresses how the current one-size-fits-all civil service system promotes equal treatment for all employees in the guise of internal equity. The most effective systems are gauged by their ability to distinguish and disproportionately reward the top performers based upon their contribution to organizational goals and objectives. Research shows that the generation now entering the workforce strongly supports this model of contribution equity. With continued

Congressional support, legislation will be passed to enable the government to more fully implement the report's recommendations.

Transition to a market-based human resource system for IT professionals that would accomplish the following:

1. Establish a market-based, pay-for-performance compensation system.
2. Allow for flexibility in the treatment of individuals and occupations.
3. Improve recruiting and hiring processes.
4. Balance the three dimensions of equity.
5. Offer competitive benefits.
6. Promote work/life balance programs.
7. Encourage management ownership.
8. Support technical currency and continuous learning.
9. Build in reliability, clarity, and transparency.
10. Implementation.

"The Transforming Power of Information Technology—Making the Federal Government an Employer of Choice for IT Employees"—National Academy of Public Administration—www.napawash.org

*Figure 6.1-2—National Academy of Public Administration
Recommendations for IT Professionals.*

CONCLUDING THOUGHTS

Many changes are needed, some internal to the DON, some requiring changes to regulations from higher authority. But regardless of the change, the overall goal must remain the same: to develop an approach that will result in a highly qualified workforce, operating in an environment that motivates them to achieve mission objectives. The DON CIO is ready to build partnerships across the Enterprise to ensure the DON has the leadership commitment, the resources, and the initiatives to develop the IM/IT workforce. With our clear vision and direction, commitment from leadership, and a willingness to invest in our people, we can shape our workforce through prioritizing work that is inherently governmental and continuing to focus on building competencies that will transform the workforce to meet today's and tomorrow's challenges

Knowledge Superiority speaks to providing power through people—what they know, how they bring their knowledge together, and how they translate that knowledge into action. To ensure Knowledge Superiority, we must engage our leaders and our entire workforce in pursuing the strategies and specific plans that will ensure the DON builds and sustains the information and knowledge-age competencies required to assure mission success. The DON CIO will continue to seek best practices from sources in the public and private sectors, and lead this effort in ways that can be replicated across Federal Government.

6.2 Integrative Competencies

Integration is a key concept for the new millennium. Integrative competencies are essential for effective decision-making in a complex world.

—Alex Bennet, Deputy Chief Information Officer, Enterprise Integration

INTRODUCTION



The exponential increase in available and accessible data and information—and the mounting pressure for the workforce to identify, assimilate, and act upon it—has led to the need to develop new skills and methods to handle this information. Integrative competencies provide connective tissue, creating knowledge, skills, abilities, and behaviors that support and enhance other competencies. They have a multiplier effect through their capacity to enrich the individual's cognitive abilities while enabling integration of other competencies, leading to improved understanding, performance, and decisions.

In this context Knowledge Management and Organizational Learning themselves can be considered integrative competencies. Because they are discussed elsewhere in this book, they are not discussed here.

An important emerging integrative competency is Information Literacy. Information Literacy is a critical life skill for today's information jungle. Being information smart means knowing how to find, evaluate, and use all forms of information. As an integrative competency, Information Literacy allows individuals to:

- Determine the nature and extent of the information needed.
- Access needed information effectively and efficiently.
- Evaluate information and its sources critically, and incorporate selected information into your knowledge base and value system.
- Use information effectively to accomplish a specific purpose.
- Understand the economic, legal, and social issues surrounding the use of information and use information ethically and legally.

Information Literacy is discussed in detail later in this chapter. Integrative competencies are also embodied in Communities of Practice (see Section 6.5, and “Systems Thinking” and “Knowing,” discussed later in this section).

SYSTEMS THINKING



Systems Thinking is one of the five disciplines of the learning organization (Peter Senge, *The Fifth Discipline*). Systems Thinking has emerged out of significant efforts by leading academics and industry executives to understand how organizations work. It is a way of thinking about, and a language for describing and

understanding the forces that shape the behavior of systems and organizations. It is about looking at the whole and moving one's focus and attention away from the pieces and the fragments; looking for the interrelationships that govern the kind of behavior and the kind of outcomes that are generated in an organization.

Systems Thinking is a way of thinking about, and a language for describing and understanding, the forces that shape the behavior of systems and organizations. It is about looking at the whole and moving one's focus and attention away from the pieces and the fragments; looking for the interrelationships that govern the kind of behavior and the kind of outcomes that are generated in an organization.

As an integrative competency, Systems Thinking expands the individual's critical thinking skills and improves both individual and group decision-making. Systems Thinking provides an approach for managing complexity in our ever increasing dynamic environment. It provides a means to understand the cause and effect relationships among data, information, and people. This integrative competency enables the individual to identify archetypes (or patterns) that occur over and over again, increasing situational understanding. Systems Thinking provides an enabling effect on other competencies through developing and integrating improved critical skills.

The continuing surge of information technology (IT) investments increases the amount of data and information available, which in turn increases the complexity of decision-making. As this complexity increases, we invest more and more in IT to help solve the problem, thereby further increasing the amount of data and information available, and further increasing, in turn, decision-making complexity. This reinforcing cycle continues.

To break this loop, the Department of the Navy (DON) is building balancing loops at the individual, organizational, and Enterprise levels. At the individual level, as decision-making complexity increases, there is a need for new cognitive skills that will allow each of us to do more with our innate capabilities. Coming out of the Massachusetts Institute of Technology's work on learning organizations, Systems Thinking skills are one way to achieve that. Systems Thinking provides an approach for managing complexity by helping decision-makers recognize and understand the cause and effect relationships between data and information. To do this, it identifies archetypes (or patterns) that occur over and over again in decision-making. In short, Systems Thinking expands individual thinking skills and improves decision-making.

Systems Thinking enables a clearer perception of the full patterns of change and the structure of systems to better comprehend their behavior and make appropriate changes. As we increase our individual skill sets in Systems Thinking, decision-making capability increases, closing the gap between decision-making capability and decision-making complexity. The middle balancing loop shows that organizational knowledge management processes (systems) improve decision-making capability (at the organization level) and the outer balancing loop says that knowledge portals do the same at the Enterprise level.

The DON has developed a multimedia course on Systems Thinking which addresses the acquisition of cognitive skills at the individual level. Available via CD and online via the Navy eLearning Network, the course provides room for the novice and those who have already been introduced to Systems Thinking to expand and test their knowledge and their ability to apply it. This virtual tool is available to all DON personnel, providing an opportunity to develop individual Systems Thinking skills.

KNOWING



It is commonly known that the world is changing at a rapid pace and in uncertain directions. This is often referred to as a non-linear, dynamic, complex world in which predictability is rare if existent at all. If we accept this hypothesis, then clearly the art of warfare in the current world environment and in the face of a new asymmetric threat can no longer rely on the logic of the past to win future engagements. As we move away from predictable warfare patterns susceptible to logic, our leaders are increasingly reliant on their “gut” instinct, an internal sense of “knowing.” To prepare ourselves to understand current situational assessments and potential enemy threats, it is essential that we learn to identify, interpret, make decisions, and take appropriate action to counter these new threats utilizing this sense of knowing.

Knowing enhances our ability to be agile and flexible at the point of action without a loss of quick response. As an integrative competency, it enhances and integrates other competencies, leading to improved decision-making. Knowing deepens our situational awareness and understanding of ourselves as well as an understanding of others, and in this context, our enemy.

Knowing is seeing beyond images; hearing beyond words; and sensing beyond appearances.

To fully utilize this sense of knowing, we must overcome three critical problem areas. The first is a thorough and deep understanding of ourselves, i.e., our goals, objectives, values, limitations, internal defenses, and weaknesses of thought and action. By knowing ourselves we learn to work within our limitations and to support our strengths, thus ensuring that the data, information, and knowledge coming to us is properly identified and interpreted. The second critical element is that of knowing the enemy. This includes areas such as culture, goals and objectives, thinking patterns, internal inconsistencies, warfare capabilities, strategies, tactics, and political motivations. Knowing ourselves and knowing the enemy is a primary theme throughout Sun Tzu’s famous master text, *The Art of War*:

So it is said that if you know others and know yourself, you will not be imperiled in a hundred battles; if you do not know others but know yourself, you win one and lose one; if you do not know others and do not know yourself, you will be imperiled in every single battle.

After understanding ourselves and working to understand the enemy, the third critical area is that of knowing the situation in as objective and realistic manner as possible,

understanding the situation in context. The current dynamics of our environment, the multiple forces involved, the complexity of relationships, the many aspects of events that are governed by human emotion, and the unprecedented amount of available data and information make situational awareness a challenging but essential phenomenon.

Traditional warfare based on command and control utilizes trained-in reactions to predetermined warfare scenarios. This approach offers quick response without much flexibility. The new knowledge warfare based on empowerment is a learned ability, developed by leaders over a period of time. The warfighting space where empowerment overlaps traditional warfare is the area of optimization and translates into agility and flexibility at the point of action without losing quick response. The knowledge and judgment capabilities of individuals at the front lines translate directly into warfighting success. Knowing ourselves, knowing the enemy, and knowing the situation, lay the framework and foundation for making effective decisions and taking the right actions, providing of course that we have built an effective warfighting capability to respond with agility and flexibility to surprise situations.

Developing the Concept of Knowing

The concept of Knowing focuses on the cognitive capabilities of observing and perceiving a situation, the cognitive processing that must occur to understand the external world and make maximum use of our internal thinking capabilities, and the mechanism for creating deep knowledge and acting on that knowledge—the Self as an Agent of Change.

Cognitive Capabilities

The cognitive capabilities for observing, collecting, and interpreting data and information, and building knowledge relative to the situation or to an enemy are: Noticing, Scanning, Patterning, Sensing, and Integrating.

Noticing represents the ability to observe around us and identify those things that are relevant to our immediate needs. We are all familiar with the phenomenon of buying a new car and for the next six months recognizing the large number of similar cars that are on the streets. This is an example of a cognitive process of which we are frequently unaware.

Scanning represents the ability to review and survey a large amount of data and information and selectively identify those areas that may be relevant. Because of the exponential increase in data and information, this ability becomes more and more important as time progresses.

Patterning represents the ability to review, study, and interpret large amounts of data/events/information and identify causal or correlative connections that over time or space may represent patterns driven by underlying phenomena which may become crucial to understanding the situation or the enemy behavior.

Sensing represents the ability to take inputs from the external world through our five senses and ensure the translation of those inputs into our mind to represent as accurate a transduction process as possible.

Integration represents the top-level capacity to take large amounts of data and information and pull it together to create meaning. This capability, to pull together the major aspects of a complex situation and create patterns that represent reality and allow one to make decisions, is one of the most valuable cognitive capabilities in warfare and management.

Cognitive Processes

The internal cognitive processes that support the cognitive capabilities greatly improve our power to understand the external world and to make maximum use of internal thinking capabilities, transforming our observations into understanding. They are: Visualizing, Intuiting, Valuing, and Judging.

Visualizing represents the methodology of focusing attention on a given area and through imagination and logic creating an internal vision and scenario for success. In developing a successful vision, one must frequently take several different perspectives of the situation, play with a number of assumptions underlying the perspectives, and through trial and error, come up with potential visions.

Intuiting is the art of making maximum use of our own intuition developed through experience, trial and error, and deliberate internal questioning and application. Intuition is typically understood as being the ability to access our non-conscious mind and thereby make effective use of its very large store of observations, experiences, and knowledge.

Empathy is the ability to take oneself out of oneself and put oneself into another person's world. The ability to empathize allows us to translate our personal perspective into that of an enemy and thereby understand their interpretation of the situation. Such intelligence is clearly advantageous in warfare.

Valuing represents the capacity to observe situations and recognize the value underlying their various aspects and concomitantly be fully aware of your own values and beliefs. Major aspects of valuing are the ability to align your vision, mission, and goals to focus attention on the immediate situation at hand, the ability to identify the relevant but unknown aspects of a situation or enemy behavior, and understanding the important aspects of the situation and being able to prioritize them and anticipate potential consequences.

Judgments are conclusions and interpretations developed through the use of rules of thumb, facts, knowledge, experiences, and intuition. While not necessarily widely-recognized, judgments are used far more than logic or rational thinking in decision-making.

The four cognitive processes—Visualizing, Intuiting, Valuing, and Judging—work with the five cognitive capabilities—Noticing, Scanning, Patterning, Sensing, and Integrating—to process data and information and create knowledge within the context of the enemy and the situation.

Self as an Agent of Change

Self as an Agent of Change refers to the internal recognition of certain factors that can influence change and the ability of self to influence or change the external world. This is the active part of knowing. Once the self has attained deep knowledge and understanding of the situation and of the enemy, this must be shared with others, accompanied by the right actions to achieve warfighting success.

The Benefits of Knowing

Some of the benefits of this power of knowing are:

- Builds situational awareness through deep understanding, having keen insight into the situation and its implications in warfighting.
- Reduces complexity by developing defenses against information and knowledge saturation and by being able to identify leverage points in the situation.
- Cultivates discernment and discretion to enable one to prioritize information and take appropriate action.
- Empowers decision-making through improved knowledge, a clear focus on the objectives, and the recognition of alternatives at the point of action.
- Supports Knowledge Superiority through building the individual's capabilities to create deep knowledge and share it with others.

Taken together, the five cognitive abilities, four cognitive processes, and elements of Self as an Agent of Change, represent the factors that can create deep knowledge, understanding, and effective actions, all necessary to obtain the real benefits of “knowing.” Each of these factors is related to many of the others, and hence it is the integrated capability built-up over time through learning, awareness, and constant self-change that creates the power of knowing, so important in the new warfighting environment.

CONCLUDING THOUGHTS



The first exposure across DON to “knowing” was embedded in the *Information Literacy Toolkit*. Subsequently this work has been widely distributed across government and was featured through the International Association on Education and Innovation in Business.

Given the DON successfully executes its holistic IM/IT/KM program, ultimately, the decision-maker's ability to navigate and productively integrate and use information comes down to the skills and knowledge of the individual; and the individual's ability to do this successfully is dependent on the relationship and networks built through collaboration, teams, and communities. This interdependence among systems, groups, and individuals is the connected world of the future, where the knowledge, skills, abilities, and behaviors of each affect all.

6.3 Information Literacy

Never in the history of mankind has so much information been available, easily available, to so many people. Our ability to function in the Navy and Marine Corps of the future depends on our ability to acquire, process, evaluate, and use information. In other words, our Information Literacy will be key to our success.

—Sandra J. Smith, IM/IT Workforce Competency Management Team Leader

BACKGROUND



Information Literacy (IL) is a set of information and knowledge age skills that enable individuals to recognize what information is needed, when it is needed, and methods for location, evaluation, use, and effective communication. Increasing IL skills will enable Naval personnel to fully exploit the technological advantages of the new millennium. The unique set of competencies of the information literate include understanding the flow of information, knowing how to assess and select the appropriate resources for information, having the skill to search for and locate needed information, being able to evaluate and interpret it, extract and organize it, and integrate and document the information. Information domains include both human and electronic sources. In today's information-saturated environment, individuals must build the sensory capabilities that are key to bridging the IL gap between themselves and the virtual dynamic environment in which the information resides.

It is estimated that the average person spends 250 hours per year looking for information. This fact represents the tremendous value of a workforce trained to quickly access, evaluate, and apply information. IL initiates, sustains, and extends lifelong learning, which enhances the individual's effectiveness in the workplace, and the world at large. IL skills are critical to dealing with the daily barrage of information, and the broad array of technologies and tools to search, organize, and analyze results, and communicate and integrate them for decision-making.

As early as 1989, a Presidential Committee on Information Literacy identified IL as a survival skill in the Information Age. The study found that instead of drowning in the abundance of information that floods their lives, information literate people know how to find, evaluate, and use information effectively to solve a particular problem or make a decision. Since that early identification of the need for IL, academic institutions have been the leaders in understanding IL issues; and working to facilitate IL in the U.S., librarians have become increasingly aware of the criticality of IL as they acquire and organize costly electronic resources for remote access. The Consortium of Naval Libraries (CNL) established its Online Literacy Working Group in 1999 to share techniques and materials on publicizing electronic resources to virtual library users and instructing them in their use.

IMPLEMENTATION



The Department of the Navy (DON) has developed the first virtual *Information Literacy Toolkit* for the U.S. Government. The DON Chief Information Officer (CIO) IL initiative builds on the CNL work with a broader effort to engender more comprehensive IL skills. It leverages national efforts, such as the Association of College and Research Libraries, *Information Literacy Competency Standards for Higher Education*, January 2000, and the American Association of School Librarians, *Information Literacy Standards for Student Learning*, 1998. It also leverages the CNL knowledge of highly relevant information resources and the decision support needs of the Department.

Fluency in IL skills will increase effectiveness and productivity of workers in searching for information and in the use of information technologies and tools. It leads to an enrichment of the knowledge base of our entire workforce. The greater goal for the IL Toolkit is to enable Knowledge Superiority and meet head-on the multifaceted decision support challenges inherent in our environment. Because as a nation we rely on the creativity, ingenuity, and intellect of people, this lends a sense of urgency to optimize the potential in every aspect of forging and honing our Knowledge Superiority edge.

The audience for the IL Toolkit is a vast and diverse population—the entire Enterprise of the DON, with coverage projected across total government—a population which possesses every gradation of knowledge, skill, ability, and behavior, and with expectations to serve a wide array of uses for the knowledge they will acquire. Employing distributed learning mechanisms is an innovative but proven way to build skills. The IL Toolkit is available via CD and on the DON IM/IT Web site. The IL team will continue to interface with Federal and other DoD groups to leverage enhancement of the toolkit. GSA has expressed an interest in this product for use on the FirstGov portal.

The IL Toolkit includes several distinctive and interrelated elements that foster the development of IL competency: a self-assessment tool, a tutorial, a navigation tool set, instructional materials, and anecdotes and links to highly relevant information resources. Another element of the IL Toolkit is Virtual Communications, which encompasses a broad spectrum of concepts, technologies, and practices central to choosing virtual tools for optimum results. Beyond the elements that directly build IL skills, the Knowing Section explores cognitive processes and capabilities required for agile and flexible response in warfare, and to engender Knowledge Superiority.

The Self Assessment helps answer the question, “How much do I know and where should I begin?” Use of a Self Assessment enables the learner to assess her own ability and isolate those areas which need improvement and growth. Part of the path to achieving IL is learning the “Big Six Skills” (Eisenberg and Johnson, 1996):

- Task Definition
 - Define the information problem
 - Identify the information needed to complete the task

- Information Seeking Strategies
 - Brainstorm all possible sources
 - Select the best sources
- Location and Access
 - Locate sources
 - Find information within the sources
- Use of Information
 - Engage in the source (read, hear, view, touch)
 - Extract relevant information
- Synthesis
 - Organize information from multiple sources
 - Present the information
- Evaluation
 - Judge the process (efficiency)
 - Judge the product (effectiveness)

Information Literacy is a set of information and knowledge age skills that enable individuals to recognize what information is needed, when it is needed, and methods for location, evaluation, use, and effective communication.

The intended outcome is to ensure all DON members can find the “right information for the right purpose at the right time.”

The tutorial builds foundational knowledge with primers from Military and academic benchmarks in IL basic standards and practices. It consists of the following tutorial sections:

Internet Primer. The Internet Primer provides basic information about the Internet, defines common terms, and explores the different types of search tools available and methods for searching. There is also a short video by Pacific Bell/UCLA on initiatives for the 21st Century entitled *Pacific Bell/UCLA Initiatives: e-literate?*

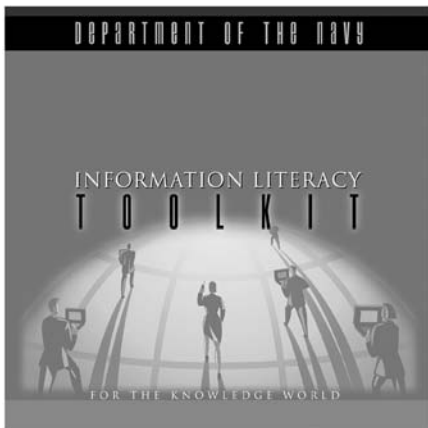
Selecting Resources. Searching for defense or Military related information on the Internet can be both easy and difficult. The Web is a vast place that is growing exponentially every day and is filled with lots of nuggets just waiting to be mined. Some are on the surface but many are down deep and require some digging. Selecting Resources covers how to select search tools and talks specifically to searching for defense and biomedical information.

Searching Resources. The Searching Resources section provides information on basic search technologies for the Web to help you understand and plan your search approach. Searching Resources will help select the appropriate search engines and directories and covers the following topics: Major Search Engines, Meta Search Engines or Metacrawlers, Directories of Searchable Databases (Invisible/Deep or Hidden Web), Virtual Libraries, The Latest in Search Tools, Internet Bulletin Boards, How Search Engines Work, Searching Techniques, Search Engine Features, and Basic Search Tips.

Evaluating Information. If you were relying on a printed newspaper or magazine for accurate information, would you place more trust in the information found in the *Wall Street Journal* or in the *National Enquirer*? Would you want to learn about cancer from Harvard Medical School or a drug company in Mexico claiming a new cancer-fighting drug? There is an amazing amount of information available on the World Wide Web, but much of it is not accurate, up to date, or even very good. Evaluating Information covers critical thinking—the procedure individuals use to make sense of and evaluate the various kinds of resources. It provides information on how to recognize computer hoaxes and urban legends, and how to evaluate and validate the information found on the Internet.

Using Information. The ability to read and use a computer to discover and retrieve information is a good start, but it is not enough. We also must be able to effectively use the information we find. Using Information covers Netiquette—guidelines that have spontaneously evolved for posting information and using the Internet. It also includes the increasingly critical areas of security and viruses, and references to links on citing electronic resources.

Information Ethics. Using information retrieved from the Internet requires responsible behavior. The intellectual property rights and privacy of information owners and producers must be respected. Proper use of information touches on some complicated and sometimes thorny issues. Information Ethics cover copyright, plagiarism, filtering or restricting access to Internet content (usually for the protection of children), and privacy of Internet users.



The *Information Literacy Toolkit* provides an ongoing resource for those who have acquired a grasp of the concepts and competencies of IL—a virtual library that enables the Sailor, Marine, or Civilian to navigate through a sea of information with the aid of specialized groupings. While there is some Navy-unique information, there are also subject guides for government, education, legal, scientific sites, technical reports, and transportation and logistics, to name just a few.

Storytelling is a powerful and evocative genre for communication. The IL Toolkit presents stories about IL that demonstrate how to solve problems by using information skills, and particularly about the power of the Internet for learning. There are Naval examples, and lessons derived from technical and educational experiences. These anecdotes foster an understanding of the need for, and utility of, IL skills.

Another element of the toolkit is a segment on Virtual Communications. Today, there's a plethora of technologies and practices that have revolutionized the way we work. How we use these tools can influence the quality of our work and can determine our ability to function as a high-producing, high-performing workforce. IL is about the ability to know and choose among the communication tools available for achieving Knowledge Superiority. Too often, organizations and individuals fail to step back and question the decision processes involved in discerning from the available options. This segment gives us a mental

decision tree about how to communicate, who to communicate with, what dimensions impact those choices, and what skills we need to communicate most effectively.

The competencies enhanced through the other portions of the IL Toolkit are brought into a different focus when we explore the cognitive process and capabilities employed in the unpredictable environment of warfare. Knowing is seeing beyond images, hearing beyond words, and sensing beyond appearances. Modern warfare demands situational awareness: knowledge of a specific situation that enables a commander to place current battlefield events into context, to share a portrayal of the situation with support staff and fellow commanders, to predict, expect, and prepare for future states and actions, and to focus on the mental or intellectual processes that result from the ability to derive expected outcomes from conscious and automatic processes such as intuition. The Knowing module of the IL Toolkit offers the opportunity to explore the way we use our thinking skills to process incoming data and information, build understanding, and drive change within ourselves and in our external environment. Knowing shows how these cognitive capabilities and processes merge the command and control of traditional warfare, where one is trained how to react, with the empowerment of knowledge warfare, where one learns the ability to optimize agile and flexible responses at the point of action. Knowing improves the ability to develop real discernment, greater associations, wise insight, and better decision-making (see the Integrative Competencies section in this chapter).

CONCLUDING THOUGHTS

Many stories can describe IL. It is an Internet search that prevents a medical emergency from becoming a tragic loss of life, or explores alternative treatment therapies and medications. It is a firefighter accessing safety information via an online database to determine precautions for his own safety in a hazardous environment, or to prevent irreparable damage to rare and precious artifacts. It is a professor who is amazed and delighted to learn how to access sites all over the world from her desktop, instead of being limited to her local library. It is the Navy doctor on a hospital ship in the Persian Gulf who is able to treat a patient locally rather than via a costly and difficult medical evacuation. It is a student using a learning program that is more than just “cool technology,” like “Quest,” which offers an online, interactive learning expedition to help a student find, recognize and evaluate content, communicate with a broad range of people, analyze information critically by weighing differing perspectives, and come to one’s own conclusions, and solve open-ended problems based on one’s research. It is the Marine sergeant from the middle of the Saudi Arabian desert using an online maintenance reporting tool to avoid a costly technical assist visit and restore material readiness and system capability with no degradation to mission accomplishment. According to former Secretary of the Army Louis Caldera, it is soldiers, comfortable in a “network-centric battlefield...where command, control, communication, intelligence, and situational awareness are accomplished digitally and shared instantaneously across the battlefield.”



The IL project is an essential tool in Enterprise integration, and will have a significant, positive impact across the Enterprise. By leveraging the power to make the most information and knowledge-rich decisions, the Enterprise will realize significant advancements in cognitive process and capabilities. To ensure Knowledge Superiority, we must engage our leaders and our entire workforce in pursuing the knowledge age competencies that are offered in the IL Toolkit.

6.4 Organizational eLearning

Organizations, as well as people, must learn to keep up with the pace of change.

—Rod French, Presidential Management Intern

BACKGROUND

Learning and knowledge go hand in hand. It took several hundred years for the most advanced nations of the world to move from agricultural to industrial to information driven economies that continue to challenge organizations to improve performance. During the past decade the new field of knowledge management (KM) has generated excitement and achieved increased visibility for its potential to leverage the newly recognized asset we call knowledge and by doing so, bootstrap organizational effectiveness. During this same decade, the notion emerged that organizations can learn and from that learning create competencies that lead to competitive advantage and agility.

The term organizational learning may refer to individual learning within the organization, the entire organization learning as a collective body, or anywhere in between these extremes. However, most organizational learning refers to team or organizational level learning. Of course, individual learning, learning in small or large groups, or as an entire organization may be needed for the firm to possess the requisite knowledge to take effective action. From a KM perspective, all levels of learning are important and all must be nurtured and made a natural part of culture. To date, most of the KM emphasis has been put on locating, creating, and sharing knowledge. For this reason, we consider organizational learning to refer to the capacity of the organization to acquire the knowledge necessary to survive and compete in its environment. However, there is an important distinction between individual learning and team/organizational level learning. Individual learning is a cognitive or behavioral activity between an individual and his environment, whereas in teams and organizations learning is a collective process dependent upon relationships and interactions among individuals such that learning occurs primarily through the interaction of the participants.

While individual learning is achieved by study, observation, cognition, experience, practice, and developing effective mental models in the mind, organizational learning, being primarily a social versus a cognitive activity, occurs when groups learn to interact, share their knowledge, and act collectively in a manner that maximizes their combined capacity and ability to understand and take effective action.

Organizational learning requires a sharing of language, meaning, objectives, and standards that are significantly different from individual learning (see Chapter 9 “Managing Change”). When the organization learns, it generates a social synergy that creates knowledge, adding value to the organization's knowledge workers and to its overall performance. When such a capability becomes embedded within the organization's culture, the organization may have what is called a core competency. These are usually unique to each organization and can rarely be replicated by other organizations. The knowledge

behind a core competency is built up over time through experiences and successes, and rests more in the relationships and spirit among the knowledge workers that is the sum of each worker's knowledge.

Organizational learning refers to team or organizational level learning. Organizational learning, being primarily a social versus a cognitive activity, occurs when groups learn to interact, share their knowledge, and act collectively in a manner that maximizes their combined capacity and ability to understand and take effective action.

Since individuals create organizations, it is they who establish the standards, processes, and relationships that enable team and organizational learning. But organizational learning is more than the sum of the parts of individual learning. For example, when individuals leave an organization, effective KM will enable the organization to retain its corporate knowledge, which is the knowledge that comes from the experience, cooperation, and collaboration of its employees.

The Department of the Navy (DON) emphasis placed on organizational learning is on learning in a virtual world, or organizational eLearning. eLearning is defined as any virtual act or process used to acquire data, information, skills, or knowledge.

THE BUSINESS CASE FOR eLEARNING

The advantages of eLearning have been recognized by government and industry alike. More than 90 percent of Cisco's training is online (*Internet Week*, Nov. 2001). Research firm International Data Corp. estimates that the eLearning market in the United States will grow from \$2.3 billion last year to \$14.7 billion by 2002. Worldwide, the overall eLearning market is expected to hit \$23 billion by 2002 (*Internet Week*, Nov. 2001).

While the costs incurred for developing an eLearning program can be significant, on the benefit side of the ledger there are well-documented cost savings associated with eLearning. These savings include reduced costs for travel, facilities, and instructors. For example, Cisco estimated it saved \$2.4 million during its first year of eLearning for every 1,000 eLearners (Giga, 2001). Likewise, the Department of Commerce commercial service division estimates that eLearning saves the division 10–30 percent in travel, instructor, and other training costs (Goodridge, June 2001).

eLearning also enables cost savings through efficiency, reduced training time, and enhanced productivity. Material presented via eLearning takes approximately 50 percent less time than classroom-style presentation. Any number of learners can receive instruction at the same time, therefore reducing the amount of training time. Finally, eLearning minimizes employee time away from the job, thus limiting employee productivity loss. These types of savings were realized at Cisco during the first year of eLearning where sales training for 8,000 people saved \$54.2 million by using eLearning rather than three weeks of classroom training (Giga, 2001).

While cost savings alone may be sufficient to justify an eLearning investment, some companies are focusing on enhanced employee job performance as a rationale for eLearning. Even though it is difficult to assess a one-to-one correlation of learning experience to performance, companies such as Shell have moved in this direction by incorporating learning in all its business unit scorecards. Ernst & Young learners and supervisors use Web-based surveys to help assess performance change and on-the-job knowledge and skill application.

The fast pace of change and a geographically dispersed workforce push learning requirements beyond the capability and feasibility of traditional classroom education. In the DON, eLearning is rapidly becoming an essential part of the fabric of continuing education needed to satisfy mission requirements.

IMPLEMENTATION



People are challenged today as never before by the rapidly changing environment in which they must function, and emerging associated competency requirements. As work becomes more and more complex, people must keep pace with new requirements being placed upon them, including understanding the way people learn through new approaches. The DON values the ability of learners to take responsibility for and direct their own learning and development, in a variety of ways and on a continual basis throughout their careers. The transformations that are changing the workplace are also expanding opportunities for people to access and acquire new learning.

Continuous Learning Guidance. Recognizing that people must become lifelong learners, especially in the area of information technology, to keep their skills current, the DON published Continuous Learning Guidance for the IM/IT workforce in July 2000. All Civilian and Military IM/IT core workforce professionals are expected to participate in at least 80 hours of continuous learning activities that augment the competencies established in their career fields and required for specific assignments. In addition to staying current in functional and professional competencies, people are expected to keep abreast of Departmental policies and programs, stay current with the management and leadership principles and practices, and pursue advanced technical, business, and managerial education and training.



Continuous learning involves everyone at every level making learning a part of their job. This shift in the way of thinking about work and learning emphasizes that learning is not restricted to traditional training and education modalities, but expanded to encompass conferences, mentoring situations, rotational or on-the-job skill development assignments, and other learning opportunities.

Meeting the dynamic needs of the DON's mission and individual career communities requires that a robust continuous education program be in place. A geographically dispersed workforce coupled with the fast pace of change push organizational learning requirements beyond the capability and feasibility of traditional classroom education. eLearning has become essential in meeting continuing education requirements. For further information, see Section 6.1 "IM/IT Workforce Competency Management."



Learning in a Virtual World. To provide learning resources for the Department, the DON CIO has partnered with the Naval Training and Education (OPNAV N79), Chief of Naval Education and Training (CNET), Naval Postgraduate School, Marine Corps Training and Education Command, and the Marine Corps Distance Learning Center to create a virtual tool on *Learning in a Virtual World*. This CD toolkit focuses on operationalizing eLearning and provides people with a single source to “learn about learning” and information on Defense learning resources. It presents a wealth of information and knowledge on the new eLearning field.

The toolkit opens with DON leaders talking about learning within the Navy and Marine Corps, and ongoing initiatives to improve education and training. Capturing these leaders’ thoughts from across key DON organizations reinforces the commitment and the importance of learning to mission performance and the future of the Department.

The first section of the toolkit focuses on defining eLearning, providing an overview with concise information on topics that include the social aspect of learning, adult learning, and learning how to learn. These complex topics are described at an introductory level in terms that are easy to understand with additional resources noted for further reading. This section also defines eLearning in terms of its relationship with Knowledge Management, Intellectual Capital, Communities and Teams, Flow, Knowing and Information Literacy.

The second section focuses on exploring eLearning in such areas as developing the business case, just-in-time learning, the ethics of eLearning, and the future of eLearning. This section also includes information on motivation and the impact of eLearning to an individual’s career. The imperative of eLearning is to ensure that DON has a qualified workforce by providing an accessible and cost effective means for people to stay current with changing requirements in today’s complex and dynamic environment. In career communities such as engineering and information technology, new developments and increasing knowledge within the industry continuously raise the professional competency standards. Meeting organizational expertise requirements necessitates that management of community, succession, and expertise be part of the same continuum, and raises the capacity to learn and change as a requirement for people to hone their skills to maintain their competitiveness.

The third section serves as a primer for operationalizing eLearning. The DON is enthusiastically embracing eLearning as a natural extension of the DON and DoD long-term commitment to education and training. Education and training is one of the primary means to sustain warfighting effectiveness and readiness, as well as to help people develop professionally and personally. While eLearning offers incredible potential for meeting increasing training and education needs for a geographically dispersed workforce, the DON must be careful as we invoke eLearning to ensure applying it in the best situations and in response to identified needs. It is not the best method for every situation despite its substantial capabilities and potential. The eLearning model presents a framework to answer these questions and develop effective eLearning. This section also includes eLearning readiness assessment instruments for individuals and organizations, information on fostering the learning organization, cost considerations and metrics, rewards and recognition, and the roles of IT, the CIO, and the Chief Learning Officer. While the intent

of this tool is not to address how to develop the instructional material, it does provide information on how to ensure a virtual learning environment adds value and highlights potential difficulties that can be encountered when developing effective eLearning instruction, including a discussion of standards, competencies, content development and delivery, and developing a community of learners.

The fourth section focuses on connecting across DON. It begins with a discussion of the current revolution in training and provides information on specific virtual training organizations and other schools in the Department of Defense.

Remaining sections include an overview on the theoretical aspects of learning—with academic discussions of areas such as intuition, attention, pattern recognition, sense making, forgetting, and balance—and a Virtual Communication section that addresses issues and opportunities arising in the virtual world of work. There is also a rich resources section filled with case studies and numerous articles and papers from industry, academic, and government contributors, and frequently asked questions and a glossary.



The DON CIO created this virtual tool specifically for use throughout the Navy and the Marine Corps, and generally for use throughout the government and by organizations supporting the government.

CONCLUDING THOUGHTS

“Overall, Federal agencies, and especially the managers in agencies, must create a learning culture”(*The Transforming Power of Information Technology—Making the Federal Government an Employer of Choice for IT Employees*, National Academy of Public Administration, 2001). People are important to the DON and increased investment in them is essential for meeting tomorrow’s mission requirements. As addressed in the Comptroller General of the United States Testimony on Human Capital in July 2001, the Federal Government is faced with a human capital crisis that can directly impact performance. Organizations can improve their ability to meet mission goals by maximizing organizational talent. Organizational eLearning is a vital component in enabling the DON to sustain and grow its human capital assets.

6.5 Communities of Practice

It was exciting working with the DON to develop the cPort virtual toolkit, the first of its kind. It is my hope that this product—reflecting much of the valuable thinking about CoPs that has emerged over the past several years—will promote successful experiences as we pursue the opportunity to create value through communities.

—Bob Turner, DON CoP Project Lead, FAA

BACKGROUND

Looking back, one hundred years from now, people will see the beginnings of a new age of connecting: people working in fascinating ways, forming networks and communities across time and distance to organize and create. All of this is taking place in a new space, the global space enabled by the Internet. All this transpiring at the new speed, the speed of thought. People working intelligently with a synergy of knowledge interaction never dreamed possible.



Communities of Practice (CoPs) are one of the first new organizational forums of the millennium. They are built on the tradition of professionals joining together to share skills and resources, and are vibrant learning centers and rich marketplaces for knowledge sharing. Etienne Wenger, co-author of the term “Community of Practice,” writes “a Community of Practice is a group of people who share an interest in a domain of human endeavor and engage in a process of collective learning that creates bonds between them” (Wenger, 2001). In a CoP research report prepared for the Federal Knowledge Management Working Group, Wenger notes three fundamental elements of this definition: (1) “share an interest in a topic” deals with the domain (Why is this important to the organization? Why would people want to participate?); (2) “interact and build relationships” deals with the community (Who should be involved? What are ways to foster trust and engagement?); and (3) “share and develop knowledge” deals with the practice (What knowledge matters? What activities are needed?).

A community of practice is a group of people who share an interest in a domain of human endeavor and engage in a process of collective learning that creates bonds between them (Wenger, 2001).

CoPs have a shared domain of practice; are aligned with the organization’s strategic direction; cross operational, functional, and organizational boundaries; are defined by knowledge, not tasks; are managed by making connections; focus on value-added mutual exchange and continuous learning; and have an evolving agenda. Critical factors for success include a sense of urgency, trust, personal passion, respect, key thought leader involvement, and open communications. Wenger states, “you cannot force a plant to grow by pulling its leaves...what you can do is create the infrastructure in which it can prosper” (Wenger, 1999).

THE VALUE OF CoPs



CoPs offer benefits to organizations, workgroups (such as teams, offices, task forces, etc.), and individuals. At the organizational level, CoPs have the ability to complement formal structures if accepted as a viable, informal way of connecting. CoPs accelerate collaboration across the organization, the rate of innovation, and the speed of quality decision-making. They leverage the organization's investment in human capital, the management of knowledge, and organizational learning. They increase performance of Enterprise portals through hosting of CoP sites, the capacity for managing complexity through the use of CoP networks, and the ability to envision the future as employee potential becomes clearer.

At the workgroup level, CoPs can support any unit where assigned work is managed to meet an organization's commitments for products and services. CoPs accelerate the use of best practices, access to just-in-time expertise, and knowledge sharing. They leverage capabilities for virtual work, access to resources, and confidence for risk management. They increase access to resources, the transfer of lessons learned, and the flexibility of work groups.

At the individual level, CoPs extend the individual's reach for knowledge, building new knowledge relationships and new access to help create a superior fighting force that is "alive with the fire of shared understanding." CoPs accelerate the transfer of know-how, collaboration, and make creative problem solving available to all. They leverage opportunities for change and growth, the capacity for knowing, and professional commitments. They increase information and knowledge competencies, just-in-time learning, and professional enjoyment.

At the heart of CoPs are new ways of recognizing and leveraging employees and the relationships they establish. For those who are actually engaged in CoPs, many community benefits will be at a higher level and more readily available than for employees, who are not engaged in CoPs but indirectly benefit from their existence. For those who depend upon CoPs, the quality of available expertise is higher, and the mode of interchange is ubiquitous (available 24/7) and virtual in that the expertise may be accessed at the actual location of work performance. In addition to all the individual benefits, at the CoP member level, there is the near-instant transfer of know-how from other members, capacity for ubiquitous collaboration, and virtual creative problem solving.

IMPLEMENTATION



Communities are flourishing across the Department of the Navy (DON). Development of an Enterprise-wide Knowledge Management (KM) Community of Practice began with two KM conferences sponsored by the DON in late 1998 and early 1999. From these early beginnings the community has grown to over 300 active participants sharing thinking virtually and in face-to-face forums held three times a year. The DON Acquisition Reform Office (ARO) is championing development of a CoP centered around Total Ownership Cost, a subject of critical importance to the defense of our country. This pilot project will be scalable for use across the Department of Defense

(DoD), and ARO is participating with the General Services Administration to expand its influence beyond DoD across government. This is only one of many government-wide pilots sponsored by the Federal CIO Council KM Working Group.

In support of the Fleet, Carrier Team One has created Knowledge Sharing Networks for the Carrier Maintenance Community that connects shipyards and ships from all over the country. In the words of a participant, people join these communities because they want to learn what other people have already learned, what mistakes have already been made, and because they want to be better at their jobs. The Pacific Fleet (PACFLT) Knowledge Management CoP is an example of a best practice community. PACFLT Knowledge Managers and leaders use the community to accelerate KM implementation and to standardize methodology throughout the Fleet to ensure the greatest impact with the least overhead. The Institute for Joint Warfare Analysis is an Innovation Community using knowledge management. Fleet Command Officers, the North Atlantic Treaty Organization (NATO), Navy Warfare Development Command, and others use KM technologies to share expertise in various technical and command and control competencies.

An early DON Community of Interest (CoI) was formed around the subject of information management/information technology (IM/IT) investment practices (see Section 8.2 “Investment Management”). This 300 plus member, knowledge-focused community carries with it a sense of urgency responding to diminishing budgets and increasing requirements, compounded by new technology insertion in a highly competitive world. As priorities shift in response to the advent of the Navy Marine Corps Intranet, the focus of this group will shift to new ways of leveraging Department IM/IT investments. The DON Navy LIFELines Services Network is a model Knowledge Stewarding community that provides information on Military medical services, crisis counseling, financial management, careers, education, deployment, and recreational pursuits. A helping community forum assists people to reach out across boundaries to connect to other people with similar interests. These are only a few examples of the hundreds of DON-related communities contributing to the mission of the Department worldwide.

An important learning with CoP and CoI implementation is that, while aligned to strategic direction, the CoP should be focused around knowledge. The strength of these communities is relationships. Focusing on respect, trust, and open communications heads a CoP down the right track for sharing and creating knowledge (see Figure 6.5-1).



To share DON successes and support CoPs as a best practice, the Department partnered with the Federal Aviation Administration and other government and industry organizations to develop and publish the first government virtual tool for building and sustaining CoPs. *Building Communities of Practice: Creating Value Through Knowledge Communities* is a guidebook for championing, developing, and participating in Communities of Practice. The guide provides a set of resources—concepts, principles, models, checklists, and tools—for building Communities of Practice. Also included are resources that can be shared with executives, champions, and sponsors, and assist community members as they establish new professional relationships to support their participation. This virtual tool has been distributed by the thousands across government and in support of government.

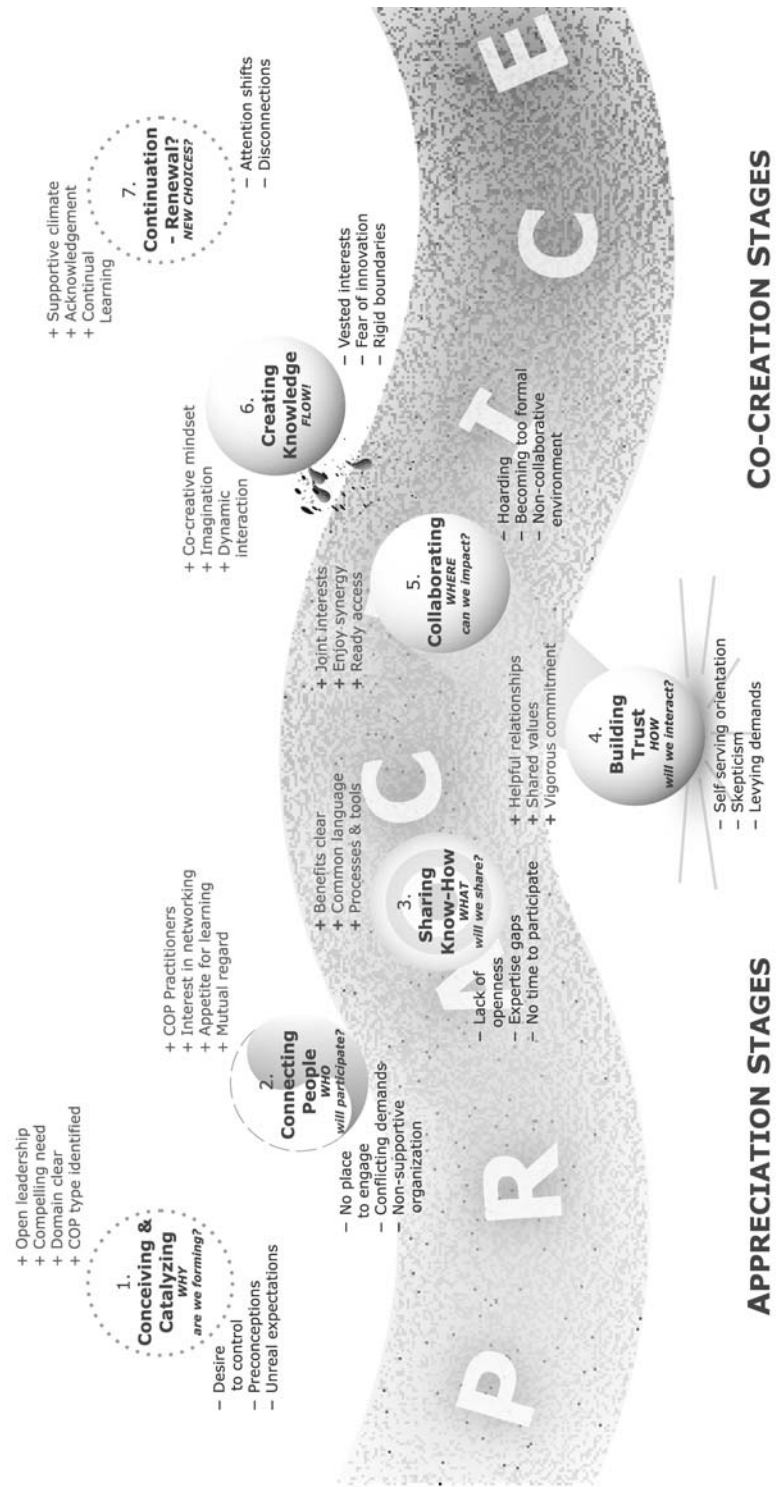


Figure 6.5-1—Community of Practice Development Model

CONCLUDING THOUGHTS

Across government, Communities of Practice and Interest are increasingly attractive as an adjunct to formal organizational processes. Organizational needs will continuously expand for knowledge access, decision support, just-in-time learning, and other knowledge worker resources in the 21st Century workplace. As this happens, we will increasingly call upon such innovations as CoPs.

6.6 Section 508

Implementation of Section 508 of the Rehabilitation Act will help break down barriers to accessing information by our employees and public customers with disabilities. In an information-driven age, improving accessibility for people with disabilities is not a matter of convenience, but rather a matter of necessity. Ultimately, everyone will benefit from this emphasis on an accessible information infrastructure; it is the right thing to do.

—John J. Lussier, Section 508 Team Leader

BACKGROUND

Section 508 of the Rehabilitation Act requires Federal agencies to meet technical compliance standards that will ensure Electronic and Information Technology (EIT) developed, procured, maintained, or used by the Federal Government is accessible to and usable by Federal employees, and Federal customers with disabilities. Section 508 applies to hardware, software, Internet and intranet systems, Web sites, and e-mail; video and multimedia; information and transaction machines such as ATM and fare card machines on Department of the Navy (DON) property; and equipment used for transmitting, receiving, using, or storing information, including telephones, fax machines, copiers, and calculators.

EIT has become an integral part of our society and plays a central and growing role in the workplace. In many ways, this evolution to an increasingly technology-centered society has provided an electronic “window on the world” to many people with disabilities, but it can present real barriers in terms of accessibility and usability. The goals for Section 508 are to: (1) eliminate barriers in accessing information technology; (2) open up new workplace opportunities for people with disabilities; and (3) stimulate the development of assistive technologies for easier accessibility. Section 508 is unique in that it is the first purely technology-based civil rights measure to be implemented by the Federal Government. As a model employer, the Federal Government needs to assure electronic accessibility for all its employees and all its customers.

CONCEPT

The Workforce Investment Act of 1998, Public Law 105–220, was enacted on August 7, 1998. Title IV of the Act is the Rehabilitation Act Amendments of 1998. Subsection 508(a)(1), as amended, requires that when Federal departments or agencies develop, procure, maintain, or use electronic and information technology, the EIT not preclude the 168,000 Federal employees with disabilities, from having access to and use of information and data that is comparable to access and use of information and data by people without disabilities. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal department or agency, have access to and use of information and data that is comparable to that provided to the public without disabilities.

A Federal agency does not have to comply with the technology accessibility standards if it would impose an undue burden to do so. This is consistent with language used in the Americans with Disabilities Act (ADA) and other civil rights legislation, where the term “undue burden” has been defined as “significant difficulty or expense.” However, the agency must explain why meeting the standards would pose an undue burden for a given procurement action, and must still provide people with disabilities access to the information or data that is affected.

In addition, a national security exception applies to any electronic and information technology used for intelligence activities, cryptologic activities related to national security, command and control of Military forces, equipment that is an integral part of a weapon or weapons system, or systems which are critical to the direct fulfillment of Military or intelligence missions. These systems do not include routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). This exception is consistent with a similar provision in section 5142 of the Clinger-Cohen Act of 1996. More specifically, the Department of Defense interprets this exception to mean that a computer designed to provide early missile launch detection would not be subject to these standards, nor would administrative or business systems that must be tightly coupled with a national security system’s architecture to ensure interoperability and mission accomplishment.

IMPLEMENTATION



Compliance with Section 508 of the Rehabilitation Act requires participation from all levels of the DON organizations. On December 21, 2000, the Access Board issued technical standards for the following six areas on Section 508:

- Software applications and operating systems
- Web-based intranet and Internet information and applications
- Telecommunications products
- Video and multimedia products
- Self contained, closed products (i.e., printers, copiers, faxes, ATMs, etc.)
- Desktop and portable computers

In addition, product support documentation and support services (including help desks) must now be made accessible.

Section 508 is essentially procurement-driven. On April 25, 2001, the Federal Acquisition Regulatory Council published amendments to the Federal Acquisition Regulation (FAR) to incorporate requirements consistent with Section 508. The following amendments took effect on June 25, 2001:

- Acquisition of EIT supplies and services must meet the Section 508 standards unless an exception or exemption applies. Exception determinations are required prior to contract award, except for indefinite-quantity contracts.

- When acquiring commercial items, an agency must identify those products and services that comply with those accessibility standards and are available in the commercial marketplace in time to meet the agency's delivery requirements.
- The requiring official must document in writing the non-availability, including a description of market research performed and which standards cannot be met, and provide documentation to the contracting officer for inclusion in the contract file.
- The micro-purchase exception (that expires on January 1, 2003) is for a one-time purchase that totals \$2,500 or less, made on the open market rather than under an existing contract.

Section 508 uses the Federal procurement process to ensure that technology acquired by the Federal Government is accessible. Beyond June 25, 2001, any time the DON enters into a contract to buy, maintain, develop, or use electronic and information technology, the products and services must comply with the Access Board standards. On or after that date, a Federal employee or customer with a disability may file a complaint or pursue civil action against the DON for failure to procure electronic and information technology that complies with Section 508. If an individual with a disability files a complaint concerning noncompliance with Section 508 against the DON, the complaint procedure established to implement Section 504 of the Rehabilitation Act for resolving allegations of discrimination in a Federally conducted program or activity shall be used. If successful in court, the individual may receive injunctive relief (e.g., the accessible technology sought) and attorney's fees, but no compensatory or punitive damages.

Section 508 does not authorize complaints or lawsuits to retrofit technology procured before June 25, 2001 in order to meet the Board's standards. However, even though Section 508's enforcement mechanisms apply only to procurement, the law does require access to technology developed, used, or maintained by a Federal agency. Further, other sections of the Rehabilitation Act require access to Federal programs (Section 504) and accommodation of Federal employees with disabilities (Sections 501 and 504). Section 508 does not apply directly to the private sector. However, contractors interested in selling EIT to the Federal Government now have an added incentive to make their products and services accessible. Moreover, the standards do not apply to technology that is incidental to a Federal contract. Thus, those products that are not specified as part of a contract with a Federal agency would not have to comply with the standards.

The Access Board recognizes that use of designs or technologies as alternatives to those prescribed in the standards may result in substantially equivalent or greater access to and use of a product for people with disabilities. An "equivalent facilitation" provision represents the realization that future technologies may be developed, or existing technologies could be used in a particular way, that could provide the same functional access in ways not envisioned by these standards. In evaluating whether a technology results in "substantially equivalent or greater access," it is the functional outcome, not the form, which is important. Through equivalent facilitation, the Access Board seeks to encourage the marketplace to offer innovative accessibility solutions.

In order to implement Section 508 successfully within the DON, we must work together as a team to deliver a consistent message to every part of the Navy and Marine Corps. DON CIO has responsibility to facilitate raising the level of Section 508 awareness throughout the Department. In February 2001, the DON 508 Working Group was created to address Section 508 implementation issues including: policy, training and outreach, acquisition, and human resource/equal employment opportunity.



The Working Group has drafted the DON CIO Plan of Action and Milestones for Section 508 implementation and compiled a directory of Section 508 resource materials. In addition, the Working Group undertook Section 508 compliance assessments of DON's "Top 20 Web Sites" in response to a Department of Justice survey request.



The Working Group also is in the process of drafting the Secretary of the Navy's Instruction on DON Section 508 Policy and has conducted a "best practices" assessment of other Federal agencies' Section 508 programs. In order to educate Department stakeholders, the Working Group decided to develop a *Section 508 Self-Help Tool Kit* CD.

The *Self-Help Toolkit* CD is designed to provide DON personnel with the full spectrum of information, procedures, resources, and contacts necessary to implement Section 508 successfully. The toolkit includes:

- Overview of Section 508.
- Overview of procurement procedures related to Section 508 implementation.
- Overview of reasonable accommodation and assistive technology.
- Accessibility guides for the six EIT categories covered under Section 508.
- Useful resources and documentation on Section 508.

CONCLUDING THOUGHTS



As we move forward and create the Department of the Navy Enterprise portal by utilizing the Navy Marine Corps Intranet and by integrating Web-enabled application systems, we must comply with Section 508 and ensure that information and data can be accessed by everyone. The end result will strengthen the Department by putting information to work for ALL our people. As President Bush stated at the Pentagon on June 21, 2001: "This is one example of the successful public-private partnerships that are removing barriers to full community participation by Americans with disabilities."

CHAPTER 7

Focus On Security

- 7.1 *Y2K*
- 7.2 *Information Assurance*
- 7.3 *Critical Infrastructure Protection*
- 7.4 *Privacy*

INTRODUCTION

The availability of timely and accurate information is an imperative in the digital age. Information technology has permeated every aspect of our organization, and is the pathway by which knowledge is gained and decisions are made. In ensuring the Nation's defense, the Department of the Navy (DON) must be assured that information is both accessible and trusted. The security of our personnel, our physical infrastructure, and our information systems are top priorities for the Department. In the wake of increased threats against the Nation's cyber and physical infrastructures, this protection mandate will only increase in importance.

Information systems are under attack. Whether from the antics of hackers or the exploits of state sponsored terrorists, the number and sophistication of attempted attacks against our networks and infrastructures is ever increasing. Successful organizations are adopting a "defense in depth" strategy to ward off these attacks and ensure the unimpeded flow of trusted information. The challenge for security professionals is that the protection of our information can stymie the collaborative eGovernment solutions that are providing such breakthroughs across our organization. In a sense, ultimate security is total isolation. This conundrum is at the heart of the challenge currently facing CIOs. The more an organization is walled away from the rest of the world, the better protected its information systems will be from viruses, denial of service attacks, etc. But in the 21st Century digital age, the focus of forward leaning organizations is on greater collaboration and interaction. Initiatives like telemedicine, telemaintenance, and distance learning not only rely upon the ability of employees to have access to information while away from the worksite, but also require active collaboration with other government organizations, industry, and academia. Unfortunately, "ultimate security" is not a realistic answer for any organization that wants to capitalize on the power of the Internet, since "isolation" is, in reality, a self-inflicted denial of service attack. Successful security solutions must embrace available technologies, but must also be based on a sound risk management strategy.

Balancing these sometimes competing agendas, the DON has given a lot of thought to "Full Dimensional Protection," reconciling the imperative for security with the imperative for change, and looking across the various components of protection to ensure that both the information and critical assets of the Department are protected, while privacy is maintained. Y2K harkened the dawn of a new awareness of the importance of information security and the availability of the information needed to run the systems upon which the

Nation depends. The impending doom forecasted by some millennium watchers galvanized large organizations like the Department of the Navy to focus on a holistic look at how information systems were integrated into every aspect of the Department's mission. And, while the dawn of the new millennium provided a brief respite from the fear of the devastation that would have resulted from the incapacitation of financial systems, utilities and transportation infrastructures, the respite was all too brief. Waves of viruses, such as "Melissa" and "I Love You," coupled with deliberate denial of service attacks on "dot com" Web sites, served to reinforce the growing realization that the information security threat was both real and undeterred by any date on the calendar.

The DON has addressed this ever increasing threat by embarking upon a comprehensive and aggressive information assurance plan. With the implementation of the Navy Marine Corps Intranet (NMCI), the Department will move from a hundred disparate networks with differing security policies to a single network and security architecture with significantly strengthened information assurance policies. Thankfully, there are a number of technological advances that will help address the information assurance challenge.

One of the most promising information security advances in recent years has been the emergence of Public Key Infrastructure (PKI). The use of PKI digital certificates is the foundation for secure eGovernment transactions and the protection of information in transit over the Internet. Digital certificates allow for the authentication of users gaining access to networks and secure Web sites, the encryption of information, and the ability to digitally sign documents and prove the identity of such signatures. Digital certificates will be the "cyber identity" of our personnel and, as such, must be in the possession of the individual and protected from compromise or unauthorized use. To ensure the protection of these certificates, the DON is leading the charge to deploy digital certificates on a smart card to all personnel within the Department of Defense. Using the smart card as the hardware token for PKI credentials avoids having to store private keys on computer hard drives, allows the individual to always have the certificates in his/her possession, and protects the certificates by the use of a personal identification number to unlock the card. The Department of the Navy is committed to the use of digital certificates to gain access to our computer network, encrypt information, sign e-mails, and access secure Web sites.

But protection of our information is only the beginning. Full Dimensional Protection is only achieved through the protection of all of the Department's critical infrastructures, both cyber and physical. The Critical Infrastructure Protection (CIP) initiative, with a mandate from Presidential Decision Directive 63 to protect the Nation's critical assets, is focused on understanding and protecting all of the critical infrastructures that the Department of the Navy relies upon to conduct its mission. The Department of the Navy's CIP initiative focuses on identifying and remediating vulnerabilities in all of the infrastructures that our bases rely upon in conducting their warfighting mission, to include transportation, utilities, telecommunications, etc. An integrated vulnerability assessment process has been created to identify single points of failure, areas of convergence, and dependencies—both on our bases and in the local communities and private sector partners—that support the Department. Building on the knowledge gained from these assessments, the Department has also developed a self assessment tool to allow Naval activities around the world to evaluate their own critical infrastructures.

However, a successful security agenda must also recognize the need to protect our personnel and ensure their rights to privacy. The incidence of identity theft is dramatically increasing, and a comprehensive security strategy must balance security requirements for information systems with requirements to protect the rights of individuals. The Department has increased its focus on privacy issues and has embraced best practices for privacy tools, such as a privacy impact assessment both to protect the rights of individuals doing business with the Department and to protect the identities of our Sailors, Marines, and Civilian employees.

Successful CIOs must balance competing interests. Nowhere is this balancing act more apparent than when dealing with security issues. Personal privacy concerns are often at odds with security imperatives. Even more importantly, successfully addressing security concerns must not be done in a manner that thwarts transformational activity and the unimpeded flow of knowledge.

There often appears to be an inherent contradiction between the goals of information assurance, infrastructure protection, and privacy. Often, efforts to secure an organization are perceived to threaten civil liberties and potentially erode the privacy of US citizens. Privacy advocates worry about increases in government secrecy and the monitoring of employees' computers. The advent of biometrics as a means of increasing cyber and physical security similarly raise concerns that the capture and storage of biometric data, if not properly managed and encrypted, would make highly personal information vulnerable to theft or fraudulent use.

A successful Full Dimensional Protection strategy must balance all of these issues. For the Department of the Navy, this strategy focuses on three key points:

- Protecting Centers of Knowledge through Critical Infrastructure Protection.
- Protecting Knowledge Pathways through Information Assurance and "Defense in Depth."
- Protecting the "Knowledge Worker" through privacy considerations.

In the 21st Century, these issues are intertwined, and physical and cyber security policies for an organization like the Department of the Navy must reflect the importance of privacy while maintaining the security needed to ensure the protection and performance of our operational forces. Systems and applications must be available; knowledge must flow. Forward leaning organizations will employ the technological advances of the 21st Century to their fullest extent, increasing mission effectiveness while ensuring the security of the Enterprise.

7.1 Y2K

Y2K highlighted the pervasiveness of information technology across our Enterprise and served as a model of how to successfully address complex organizational challenges in the 21st Century digital age.

—David M. Wennergren, Deputy Chief Information Officer, eBusiness and Security

BACKGROUND

As countdown clocks around the world focused attention on the coming of the year 2000 (Y2K), prognosticators of doom predicted the end of civilization. At a conference in Washington, DC, university professors and industry leaders evoked visions of martial law, as the “Y2K bug” wrought havoc with information systems and devices throughout the world that relied upon embedded computer chips. In the suburbs of Virginia, a newspaper article spotlighted a family stockpiling Spam and Velveeta to survive the breakdown in society that they deemed inevitable.

As a global Enterprise with roughly 800,000 Civilian and Defense personnel, more than 200 installations, 315 ships and 4,000 aircraft, hundreds of thousands of infrastructure systems, and an annual budget of \$82 billion, the Department of the Navy (DON) faced a daunting Y2K challenge. The nature of Y2K did not allow for extensions, so technology and management practices had to be synchronized.



The Department’s challenges centered on developing an Enterprise effort to solve Y2K issues, while at the same time continuing to support the requirement to maintain a global Naval presence. A centralized policy with a decentralized execution strategy was the only path to success. The challenge was to create an organization and a management structure that allowed our Military commanders the autonomy to perform their missions, but also to provide a centralized direction for the Y2K certification of thousands of major systems and hundreds of thousands of infrastructure devices.

IMPLEMENTATION



The DON met the challenge with an innovative combination of management processes, leadership, and tools. Senior leadership had a hands-on approach to the Y2K effort, driving the teams to focus on and achieve program objectives. The Navy and the Marine Corps Y2K teams at the headquarters level and out in the Fleet and in the field accomplished the lion’s share of the Y2K work. The Department also enlisted public and private sector experts to build a store of knowledge in numerous aspects of technology and management disciplines.

Leading this Y2K mediation effort, the DON Chief Information Officer (CIO) adopted a five-phase management approach, which was endorsed by the General Accounting Office and recognized by Congress. Each of the phases had target completion dates and exit criteria that had to be passed before moving to the next phase.

Awareness Phase. Familiarize DON personnel with the scope of possible Y2K impacts, define the problem, establish compliance standards, decide on overall approach, and obtain high-level management support. Actions for this phase included identifying points of contact and assigning responsibilities, publicizing the DON Y2K Web site, setting up a help desk and Tiger Teams, establishing compliance standards, sharing success stories, and conducting program reviews. During this phase the DON held a Virtual Town Hall to address the Department's Y2K concerns. DON leaders were on hand to discuss Y2K issues and answer Y2K questions from a live audience. This event, broadcasted live via satellite to Naval activities around the world, was a major step in providing awareness of what the Department was doing to prepare for Y2K.

Assessment Phase. Determine the impact of Y2K on DON's inventory of artifacts, including, but not limited to, systems, tools, products, workstations, and contracts; and develop acceptable solutions, resource estimates, tool needs, risks, contingency plans, and project plans for fixing Y2K impacted artifacts. The actions associated with the phase included creating an inventory of all systems, tools, products, workstations, embedded systems, etc., identifying all interfaces and tools, establishing support teams to assist with assessment and using proven assessment methodologies in assessing artifacts, conducting pilot program, identifying technical issues, and conducting risk analysis and contingency planning.

Renovation Phase. Develop the actual correction of the Y2K problems in each system. Actions for this phase included ensuring Y2K compliance in both new solicitations and existing contracts; purchasing only Y2K compliant products; identifying and implementing solutions and determining a suite of acceptable solutions for DON systems; retiring, replacing, and rewriting impacted systems; and maximizing information sharing to reduce duplication effort.

Validation Phase. Test and verify the correctness of the renovated or replaced system. This included all traditional types of testing such as regression, integrated, and simulation testing.

Implementation Phase. Field the renovated or replacement system, put in place backup and recovery plans, and ensure coordination with other systems and databases to provide for seamless interfaces.



The Department Y2K effort included the remediation of 663 mission critical and 1,461 mission support systems. The effort to ensure the readiness of shore infrastructure included cataloging 924,825 devices—such as local area networks, servers, faxes, and heating equipment—at more than 200 major installations located inside the United States and in other countries. While individual system developers worked hard to remediate code, facilities managers researched the status of embedded chips, and disaster recovery planners exercised contingency plans. DON Y2K actions encompassed all the efforts required to plan for, live through, and learn from the transition to the year 2000. The DON goal was not only to ensure that our operating forces transitioned seamlessly into the next millennium, but to use our Y2K investment for long term advantage.



The Department of the Navy focused on much more than just the identification and correction of specific “date problems.” DON leaders recognized early on that the concern over Y2K was one that would affect everyone, both at work and at home. Embarking on a robust awareness campaign, the Department used Web sites, brochures, videos, and public service announcements to drive home its message about the myths and realities that might confront individuals in the New Year. The Department conducted an Industry Forum to share best practices and strategies with industry leaders. An Expert Forum was also conducted, bringing together thought leaders from a diverse set of disciplines to think through issues of consequence management, identifying the unintended consequences of potential actions, and developing strategies to recognize and then address the impacts of unforeseeable issues. A Y2K Virtual Town Hall was held, bringing together Naval commands from around the world via satellite, telephone, fax, and Internet streaming. Navy and Marine Corps senior leaders were on hand to discuss Y2K issues and answer questions from a live audience. This event was a major step in providing awareness of what the Department was doing to prepare for Y2K.

Fortunately, through the hard work of DON professionals around the globe, the new millennium entered quietly, Y2K came and went, and society turned its attention to other matters. The Department of the Navy, deployed around the globe, successfully ushered in the New Year, time zone by time zone. The USS Topeka, a submarine deployed at the International Date Line reported all was well as New Year’s Day officially began. In Singapore, the USS Bremerton, another submarine, reported in on national television. Naval base commanders in the Pacific and Europe similarly reported all was well. And in a true display of the pervasiveness of information technology (IT) in our society, an aircraft carrier deployed in the Persian Gulf broadcast live on MSNBC, via Internet streaming, its crew ringing in the New Year.

Y2K was the last major information security initiative of the 20th Century, and became a model on how to deal with complex organizational challenges at the dawn of the 21st Century. Y2K taught us a lot about information technology. We became aware of the ubiquity of technology in our lives. As that awareness grew, it became clear that IT was no longer solely the domain of information technology professionals in raised floor computer rooms. Instead, IT had become a complex web that ran through every major weapons system and every major sector of our economy. The Y2K challenge crossed all boundaries; organizational, national, and cultural. The Y2K challenge changed the way that management thought about and dealt with technology related problems. The turning point for most organizations, as they strove to address their Y2K concerns, came when they realized that Y2K was a “CEO issue,” not just a “CIO issue.”

Y2K LESSONS LEARNED



There is much that can be learned from the Y2K experience, including the importance of working across organizations and functions to solve problems, ensuring awareness, focusing on consequence management and continuity of operations, understanding the relationships and interfaces between systems, and considering the unintended consequences of actions. Many of the actions taken to ensure the successful 2K transition offer continuing value in helping the Department address other

large scale, complex issues. Preparations for Y2K highlighted the importance of accurate asset inventories, configuration management, and a complete understanding of all of the interfaces that exist between complex systems. Y2K preparations in the Department of the Navy also resulted in complex interrelated testing strategies never before considered. Entire Carrier Battle Groups and Amphibious Readiness Groups operated at sea with their clocks rolled forward to January 1, 2000. Entire groups of logistics systems and personnel systems across the entire Department of Defense were similarly tested. These new and enhanced testing strategies did much more than just identify Y2K date anomalies that had not been successfully remediated; for every one potential Y2K problem uncovered, up to ten other interoperability problems were identified and addressed. These more robust and interactive testing strategies have been institutionalized as part of the pre-deployment preparations of our operating forces.



Figure 7.1-1—Y2K Town Hall

CONCLUDING THOUGHTS

One of the most lasting lessons learned of Y2K is the need to focus on consequence management. The value of contingency, disaster recovery, and continuity of operations plans was highlighted, and the insights gained from these preparations continue to have value across our Enterprise. Planning for continuity of operations ensures the security and availability of our networks, the mission capability of our operating units and weapons systems, the availability of public utilities, transportation networks, and telecommunications systems, and the protection and restitution of our critical infrastructure assets. January 1, 2000, was a quiet day; but the lessons learned from Y2K will enhance the protection of our personnel, facilities, and systems for years to come.

7.2 Information Assurance

Information is one of our most important resources. To ensure the success of our mission, we must ensure the availability, accuracy, and timeliness of our information.

—CAPT Sheila McCoy, USN, DON CIO IA Team Leader

BACKGROUND

The National Security Telecommunications and Information Systems Security Committee (NSTISSC) defines information assurance (IA) as “Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.” IA is making sure users have the correct data when they need it, and people who shouldn’t see it can’t.

The Department of Defense (DoD) is increasingly dependent upon a commercially based global information environment over which it has little control, thereby increasing its exposure and vulnerability to a growing number of sophisticated internal and external threats. Today’s Internet-linked information systems create a new dimension for warfare, making it possible for a single adversary gaining access to a single network connection to surreptitiously disrupt many systems and networks. Once inside a system, an adversary could exploit not only that system, but also all systems networked to it. This threat to information systems is constantly evolving, and in the wake of terrorist acts on the U.S. homeland, awareness of this threat has increased and many security experts predict that these attacks in cyberspace will increase even further. Indeed, since September 11, 2001, the Internet has seen an increase in intentional disruptions of service by those wishing to express their views about the global war on terrorism.

The Government Information Security Reform Act (GISRA) of 2000 requires that each Federal agency, including the DoD, monitor and implement information security practices. The DON Chief Information Officer (CIO) works with the DoD CIO to meet these objectives. The DON CIO develops IA vision, strategy, and policy for the Navy and the Marine Corps.

IMPLEMENTATION

Implementing IA requires using the right tools at the right time along with the active involvement of every individual who has the need to access information, including DON staff, contractors, and vendors. Risk assessment includes not only identifying each potential vulnerability and determining the probability of an exploitation of that vulnerability, but also the potential damage due to such exploitation. Following risk assessment is application of a measured strategy to mitigate risks, by technology, procedure, or training. This process of risk analysis and mitigation is known as risk management. Specifically, risk management is the “Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment.” (NSTISSC)

Information Assurance is defined as “operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.” (NSTISSC)

Risk management is a key to a successful IA strategy. While information stored on a computer that is disconnected from networks, powered off, and locked in a room with no key is well protected from any attack, it is also unavailable to individuals who have a legitimate requirement for that information. Information must be readily available to authorized users while the risk of that information becoming available to adversaries is minimized. Dedicated networks for limiting access have been used successfully to protect classified data. However, the cost to maintain separate dedicated networks while ensuring access to distributed users (both within and external to the DON) is potentially too high for unclassified systems. Instead, unclassified systems rely principally on encryption and access control to maintain data availability while ensuring confidentiality.

Because there is no “one shot” solution to ensure security, DoD has developed a multitiered IA strategy, called “defense in depth,” to ensure the security of our Military’s computer networks. With the defense in depth approach, network boundaries are protected by layered implementation of IA tools as shown in Figure 7.2-1.

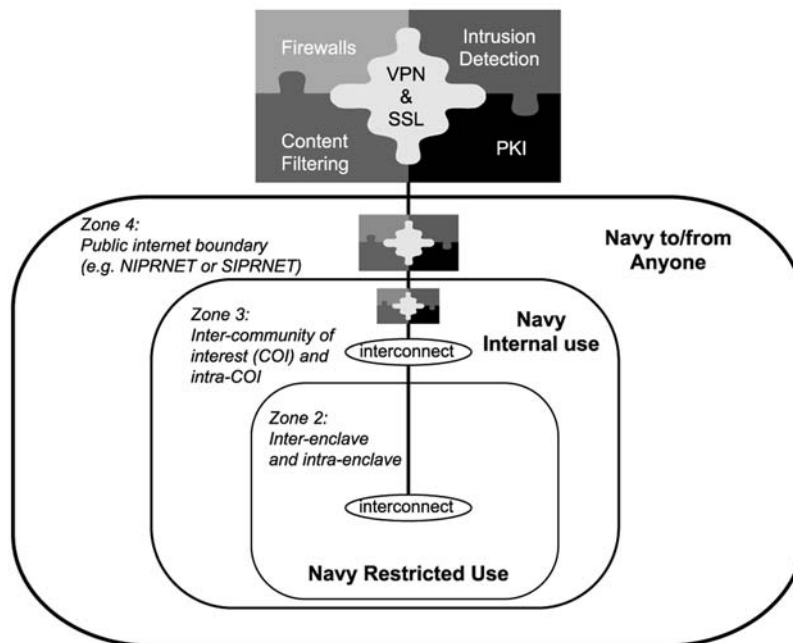


Figure 7.2-1—Layered implementation of IA tools protects network boundaries and is part of DoD’s defense in depth approach.



Because of the interconnected nature of the Global Information Grid, a risk assumed by anyone, at any level, is a risk assumed by all. IA is therefore necessary at all levels. That goal can be achieved through defense in depth, which employs mechanisms on successive layers at multiple locations. The “weakest-link” analogy is often used to illustrate the significance of network security. The defense in depth approach makes it more difficult for an attacker to gain access. The attacker would have to locate and exploit multiple holes in each layer before obtaining access to his target rather than just targeting the single weakest point in the network.

Components of this strategy include personnel, technology, and operations. The Department will continue to test the effectiveness of IA initiatives in these areas through audits, vulnerability assessments, online surveys, and red-teaming.

Personnel

People using technology to conduct operations form the central element of defense in depth. People design, build, install, operate, authorize, assess, evaluate, and maintain protective mechanisms. To enhance IA through personnel we use training and certification programs. DON CIO requires all members of the Department to undergo annual user training, with a concentration on Internet security risks and practices.

Technology

To conduct an effective cyber-defense, DoD must have a well-stocked collection of tools and the skills to use them. There are many tools that have been developed and implemented to assist in meeting IA requirements. The table in Figure 7.2-2 lists some of these tools and the objectives they support.

OBJECTIVE	TOOLS
Availability	<ul style="list-style-type: none"> • Redundant Arrays of Independent Disks (RAID) • Redundant power supplies • Server clustering • High-speed network backbones • Content filtering
Data Integrity	<ul style="list-style-type: none"> • Digital signatures • Encryption including Secure Sockets Layer (SSL)
Authentications and Authorization	<ul style="list-style-type: none"> • Firewalls • Virtual Private Networks (VPN) • Public Key Infrastructure (PKI) digital certificates • Passwords • Access control lists
Confidentiality	<ul style="list-style-type: none"> • Intrusion detection • Firewalls • Encryption including Secure Sockets Layer (SSL)
Non-Repudiation	<ul style="list-style-type: none"> • Digital signatures • Audit logs

Figure 7.2-2—Many tools have been developed and implemented to assist in meeting IA requirements.

Tactics used to defend the network and infrastructure include the use of multiple and redundant data paths to allow more than one physical medium or route for data transport. This tactic counters the physical loss or damage of one transmission medium or path.



DON CIO continues to lead in applying the Department's defense in depth strategy at our network boundaries through the use of intrusion detection systems to identify and prevent unauthorized network access. DON uses anti-virus protection software installed at various levels in the network to block known malicious code.

One specific example of DON CIO use of IA technology is our firm commitment to the DoD Public Key Infrastructure (PKI). PKI is a technology that permits secure transactions to occur without the limitations of traditional key exchange systems. Under the old symmetric keying systems, users desiring to communicate securely needed to possess a shared secret that had to be delivered by a trusted source on a channel other than the one they would use for the communication. With PKI, each user is given a pair of mathematically related keys. One is kept secret (private) and the other is published (public). When two users need to communicate securely, one simply obtains the public key belonging to the other from a trusted source. The public key is then used to encrypt the message and the receiver then uses his private key (which only he possesses) to decrypt it. A reverse of this technique can be used to validate the origin of a communication.

The DoD PKI will greatly enhance our ability to protect the confidentiality of our data and provide a means to ensure data authentication and nonrepudiation of receipt or delivery. Under the DoD plan, all personnel (active duty, selected Reservists, Civilian DoD employees, and on-site contractors) will be issued PKI digital certificates.



The Department of the Navy was instrumental in leading the charge to ensure that digital certificates used to access unclassified information will be contained on the DoD Common Access Card (CAC), which is a smart card that will replace the current Military ID. PKI will be used to digitally sign and encrypt communications, identify the individual to Web sites, and grant access to unclassified DON IT resources on the network.

Operations

IA policy drives IA operations by establishing goals, actions, procedures, and standards. To prevent the potential breakdown of barriers and the invasion of the innermost (or most valuable) parts of a system, defenses must be constructed in successive layers and by setting safeguards at various locations. In addition, DON CIO is implementing a policy that will require comprehensive contingency planning for all DON mission critical systems.

As a major operational element of the defense in depth strategy, the DON has launched a new Enterprise network, Navy Marine Corps Intranet (NMCI). NMCI will promote IA goals by limiting interfaces to external less controlled networks, standardizing network configurations, ensuring high-speed availability, and enforcing DoD and DON policies. The NMCI will be contractor-provided and operated through an innovative seat

management contract. Information security and computer network defense are built into the contract in a way that gives the contractor incentives for good performance. This performance will be assessed not only by inspection but also by how well the contractor responds to unannounced attacks from DON red-teams. The NMCI will bring together the hundreds of disparate DON networks under a single security architecture and framework, significantly improving the Department's IA capabilities.

LOOKING FORWARD

Implementing PKI and NMCI are just two of the steps in the long-range plan to transition information systems from stand-alone, stovepiped, non-interoperable systems into global end-to-end integrated, networked, tactical, and tactical support systems. As the transition provides increased authorized access to information using standardized tools and interfaces, advanced tools will be integrated into those interfaces to detect and prevent unauthorized access. This unified well defended architecture will support the needs of the DON today and into the future.

Today you carry around tokens that identify you and provide you authorized access to the physical world. Your keys open doors. Your credit cards let you purchase goods and services. You accept the inconvenience of having to carry keys and credit cards because you can see the benefit of controlling access to your property and money and yet having access when you need it. In the future—a future that is technologically possible today via smart cards and other similar technologies—you will carry around tokens, possibly future versions of the same tokens you have now, that will also unlock your access to the virtual world. Your tokens carry private keys that correspond to digital certificates issued by a trusted PKI. They may also contain biometric templates that associate the token to your physical characteristics. These tokens will unlock physical doors and provide logical or virtual access to information.

In this new world, IA is integrated into all networked systems, allowing for transparent cross-linking of information across multiple data sources, while maintaining data protection and strong authentication of who is accessing that data. Here is a sample morning.

WHAT DOES SUCCESS LOOK LIKE?

You go to work. As you enter the turnstile at the building where you work, your smart card-based identification card identifies you as an authorized employee to the access control database. (By linking access control to a networked system, creating a forgery of the physical smart card will not be sufficient for the adversary to gain access.) When you arrive at your desk, you discover that your workstation is not functioning properly. You contact the help desk, which provides you with a temporary workstation while yours is repaired. You use the PKI private key on your smart card to authenticate to the temporary workstation. Your identity credentials are forwarded to the network, which in turn downloads your settings to the workstation, allowing you access to all of your network-stored information. (By requiring digital certificates for access to your network settings, only you will be able to access them.) Your morning project requires accessing information from three data sources,

all of which are available on the Internet. You access all three sources using your private key from your smart card to authenticate your identity and unlock access. (Since all information is encrypted in transit over the Internet, and your private key was required to initiate access, the adversary cannot spoof your identity or “listen in” to the data transfer.)

You receive a phone call from the building security desk. There is a visitor who claims to be there to meet you. You realize that you forgot to enter the visit authorization for your 10:00 appointment. You quickly pull up your contacts list, authorize access for today for the individual, and then tell the security officer that the visitor should now be recognized. The visitor uses his smart card and is granted access. (Since building access control is linked to the network identification system, only the real individual you are expecting will be permitted access. An imposter will not have the correct credentials.)

As you leave for lunch, you remove your smart card from the workstation, locking all access to the workstation and blacking out the screen. You activate your wireless personal digital assistant with your smart card to ensure you receive immediate notification of any messages for you while you are out of the office. (Since your smart card is required to activate the wireless device, loss of the device will not result in a security breach. Since all wireless transmissions are encrypted, the adversary cannot listen in on data transactions.)

In this not so future scenario, all access was monitored and required the use of proper digital credentials. However, because of the integration of IA tools, most of the protection of data was transparent to the user. IA served as an enabler, rather than a deterrent for the authorized user, while providing effective barriers against information loss or disclosure to unauthorized parties.

7.3 Critical Infrastructure Protection

As the Department's Critical Infrastructure Assurance Office, our primary mission is to be integration agents across the Enterprise. Our goal is to get outside the "fenceline" and look at our infrastructures in a broader context.

—CDR Lynne D. Gaudreau, USN, DON CIO CIP Team Leader

BACKGROUND

The world has changed dramatically since the days of the black and white, bipolar balance of power that shaped our defense efforts from the end of World War II to the fall of the Berlin Wall. We now face a new, much more insidious threat, known as asymmetric warfare. This new brand of warfare is unconventional, and brings an added danger of being possible not only via large or small bands of terrorists, but even by just a single person with a computer and modem. The credibility of this threat has become shatteringly real in the wake of the September 11, 2001 attacks against the United States at the World Trade Towers and the Pentagon.

Asymmetric warfare has the attention of the highest levels of the Department of Defense (DoD):

I would say that the so-called "asymmetrical" threats constitute more significant threats today than the risks of a major land, sea, or air war, where some country decides to threaten Western armies and navies and air forces. I think that the threats of terrorism and cruise missiles, as well as ballistic missiles, information warfare, are all things that we need to be attentive to.

- Secretary of Defense Donald Rumsfeld
March 8, 2001 News Briefing

As the threat has grown in complexity, so has the business of national defense. Today, our defense environment includes the following realities:

- More of what were "inherently governmental" activities are being transferred to the private sector. Over 90 percent of the services required for day to day and warfighting operations of defense components come from the private/commercial sector.
- Mergers and acquisitions within the international defense industry have led to the globalization of weapon systems sustainment.
- Old defense mechanisms are no longer sufficient.

These realities, with the increasing potential for asymmetric/unconventional warfare, led to the development of Presidential Decision Directive (PDD-63) titled "Critical Infrastructure Protection." PDD-63 recognized the "growing potential vulnerability" of "physical and cyber-based systems essential to the minimum operations of the economy and government." PDD-63 established a "national goal" to: (1) institute a comprehensive

program to identify critical infrastructures (public and private); (2) assess their vulnerability to being taken out of service; and (3) institute a method for mitigating the risk to those infrastructures.

It is from this mandate that a national Critical Infrastructure Protection (CIP) program was officially initiated. The Department of the Navy (DON) CIP program has been designed to support the operational readiness of its warfighters through the development and administration of an effective, Enterprise-wide CIP program. This program builds upon the Department's longstanding antiterrorism/force protection programs and includes the newer cyber security programs of information assurance.

Critical Infrastructure Protection is defined as the identification, assessment and assurance of cyber and physical assets essential to the mobilization, deployment, and sustainment of Naval warfighting operations.

DON CIP GOALS

The goals of the DON CIP program are to:

- Ensure the development of an integrated CIP capability.
- Support the development of Sector Assurance Plans.
- Integrate the efforts of other related DON programs into CIP.
- Support the development of an integrated indications and warnings capability.
- Establish a Web-based clearinghouse for DON CIP specific information and guidance.
- Establish long-term programmatic objectives for DON CIP.

The ultimate objective is a functioning CIP capability that provides DON warfighters with the assurance that infrastructures on which they depend will be available when needed.



The DON CIP program is an Enterprise-wide partnership of organizational entities that are essential to achieve effective protection of critical infrastructures.

The term infrastructure includes systems and assets that enable the DON to accomplish its warfighting mission and core business processes. The DON CIP program leverages integrated physical/cyber and on/off-base infrastructure protection strategies to enhance the protection of DoD/DON mission essential infrastructures upon which the availability and readiness of our Military forces depend. Key participants in this mission include the Office of the Department of the Navy Chief Information Officer (DON CIO), Navy and Marine Corps Sector Leads, Navy Criminal Investigative Service (NCIS), and the Joint Program Office for Special Technology Countermeasures (JPO-STC).

PRIMARY ISSUES

Defining Which Infrastructure Assets are Most Critical

Though critical, not every asset needs to be protected to the same degree. DON CIP efforts focus on the most critical infrastructure assets. DON CIP adopts the following tiered view of criticality (initially developed by the Office of the Secretary of Defense):

- **Tier I:** Warfighter suffers strategic mission failure. Specific timeframes and scenarios assist in infrastructure prioritization.
- **Tier II:** Sector or element suffers strategic functional failure, but warfighter strategic mission is accomplished.
- **Tier III:** Individual element failures, but no debilitating strategic mission or core function impacts occur.
- **Tier IV:** Everything else.

Protecting Critical Infrastructures

The concept of protecting those critical infrastructures necessary to ensure mission success (i.e., vulnerability identification and remediation) focuses initially on single-point failures, and then expands beyond into double, then triple-point failures. Protection and risk acceptance decisions rest primarily in the hands of infrastructure owners and installation commanders. Successful CIP means influencing these risk acceptance and protection decisions.

The DON CIP Working Group ensures compatibility of approaches within each of the various protection activities and across Defense Infrastructures sectors. In fact, a primary responsibility of the Working Group is to oversee the full range of CIP protection activities described in Figure 7.3-1. The DON CIP Working Group plays an important role in coordinating, and in some cases, leading various elements of the protection activities.

FOCUS

The DON CIP focus is to reduce the risk to DON strategic Military mission accomplishment through a three-step process. This process consists of: (1) enhancing DoD/DON's understanding of critical infrastructure dependencies; (2) mitigating critical infrastructure vulnerabilities; and (3) applying an Enterprise-wide risk-based management framework, considering physical and cyber vulnerabilities to government and commercial critical infrastructures, to assist in Enterprise-wide, risk acceptance decisions.

The initial emphasis is to identify and mitigate existing Tier I and Tier II vulnerabilities in order to provide the most significant and immediate benefit toward providing Military mission assurance and improved operational readiness. As perceived threats and opportunities arise, DON CIP increases emphasis on the Consequence Management phase of CIP activity. This strategy is consistent with the intent of PDD-63 to ensure critical infrastructure protection, and melds well with both the PDD 67 focus on continuity of operations and the antiterrorism emphasis of PDDs 39 and 62.

VISION

The DON CIP vision is to significantly improve DoD/DON's operational capability and readiness by fully integrating DoD/DON CIP efforts. For DON CIP to succeed, every DON infrastructure owner must understand the importance of their critical infrastructures to DoD/DON mission accomplishment, and manage their critical infrastructure dependencies and risk through the conscious application of an Enterprise-wide, risk-based management framework.

To achieve this vision, the Department has developed coordinated physical/cyber and on/off base critical infrastructure protection strategies, leveraging a variety of ongoing analyses, assessments, and protection efforts into a coherent, integrated CIP process. The DON CIP process consists of the following:

- Physical security analyses and assessments.
- Operational security analyses and assessments.
- Antiterrorism/Force Protection analyses and assessments.
- Cyber protection and vulnerability analyses and assessments.
- Organic (government) and non-organic (commercial) infrastructure vulnerability and dependency analyses and assessments.

OPERATIONAL STRUCTURE

PDD-63 divides government functions into service "sectors" such as information and communications, banking and finance, water supply, etc. Lead Agencies report to the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, US Government sector. As stated in PDD-63:

"Lead Agencies" are to develop individual CIP Programs to meet a self defined Initial Operational Capability (IOC) by the end of calendar year 2000, and a Full Operational Capability (FOC) by May 21, 2003.

According to PDD-63, the DoD performs a "special function" of government, and is responsible to develop its own Enterprise-wide CIP Program in cooperation with the national leadership. The DoD CIP Plan was released November 18, 1998. CIP leadership in the DoD rests with the Assistant Secretary of Defense for Command, Control, and Communications (ASD (C3I)), who carries the title: DoD Critical Infrastructure Assurance Officer (CIAO). In the Department of the Navy, the DON CIO is designated as the Critical Infrastructure Assurance Officer.

By a memorandum dated August 26, 1999, the Under Secretary of the Navy identified the DON CIAO and established the DON CIP Council. DON CIP Council members are provided in Figure 7.3-2.

To facilitate DON responsiveness to DoD CIP programs and for implementing DoD and DON CIP initiatives, DON CIO has dedicated resources to administer the DON CIP effort, creating a working group of subject matter experts reflecting the CIP sector construct. This group is the DON CIP Working Group. Its members are presented in Figure 7.3-3.

Critical Infrastructure Protection Activities	
Protection Activities	Description
Infrastructure Analysis and Assessment	Coordinated identification and characterization of DON, DoD, National, and International critical assets, their system and infrastructure configuration and characteristics, and the intra/interdependencies within and among infrastructure sectors; assessment of their vulnerabilities; quantification of the relationship between military plans and operations and critical assets/infrastructures; and assessment of the operational impact of infrastructure loss or compromise.
Remediation	Deliberate preventative measures undertaken to improve the reliability, availability, and survivability of critical assets and infrastructures (e.g., emergency planning for load shedding, graceful degradation and priority restoration; increased awareness, training and education; changes in business practices or operating procedures, asset hardening or design improvements, and system level changes such as physical diversity, deception, redundancy and backups).
Indications and Warning	Tactical indications through the implementation of sector monitoring and reporting, strategic indications through Intelligence Community support, and warning in coordination with the National Infrastructure Protection Center (NIPC) in concert with existing DoD and national capabilities.
Mitigation	Preplanned and coordinated reactions to infrastructure warning and/or incidents designed to reduce or minimize impacts; support and complement emergency, investigation, defense, or other crisis management response; and facilitate reconstitution.
Response	Coordinated third party emergency (e.g., medical, fire, hazardous or explosive material handling), law enforcement, investigation, defense, or other crisis management service aimed at the source or cause of the incident. Response to infrastructure incidents involving Defense infrastructure will follow one of two paths: (1) affected Components and/or the Joint Task Force for Computer Network Defense (JTF-CND) will defend against and respond to all cyber incidents in accordance with granted authorities and established operational procedures, or (2) affected Components will defend against and respond to all non-cyber incidents in accordance with granted authorities and established operational procedures.
Reconstitution	Owner/operator directed restoration of critical assets and infrastructure.

Figure 7.3-1—DON Critical Infrastructure Protection activities.

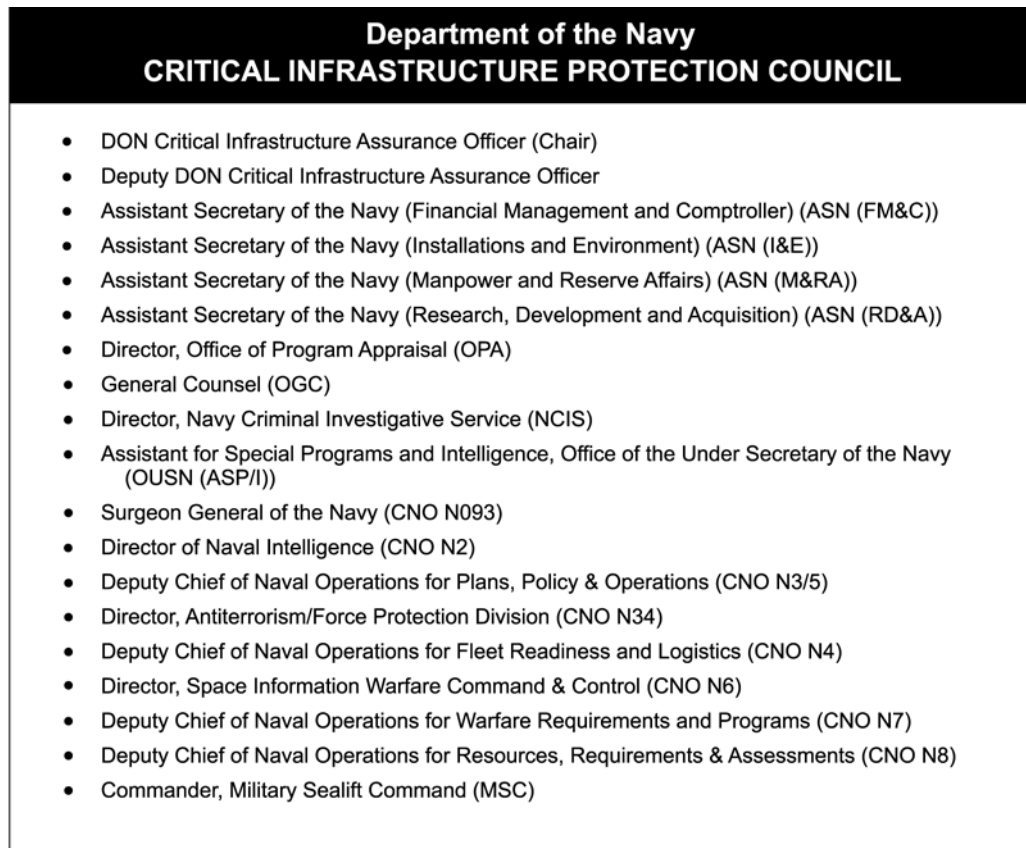


Figure 7.3-2—The DON CIP Council was established by the Undersecretary in August 1999.

Department of the Navy CRITICAL INFRASTRUCTURE PROTECTION Working Group	
Functions	Navy & Marine Corps Leads
Chair	<ul style="list-style-type: none"> • DON CIO Team Leader for CIP
Indications and Warning	<ul style="list-style-type: none"> • Director, Requirements, Plans, Policy and Programs Division (CNO N20) Intelligence Plans and Policy Branch (USMC I) Naval Criminal Investigative Service
Assessments	<ul style="list-style-type: none"> • Anti-Terrorism/Force Protection Division (CNO N34) Homeland Defense Branch (HQMC PSH) Fleet Information Warfare Center Marine Corps Information Technology Operations Center Joint Program Office for Special Technology Countermeasures
Service Sectors	
Personnel	<ul style="list-style-type: none"> • Assistant Secretary of the Navy for Manpower and Reserve Affairs Bureau of Naval Personnel (Pers 074) Manpower (HQMC M&RA)
Health Affairs	<ul style="list-style-type: none"> • Director, Medical Resources, Plans and Policy Division (CNO N931)
Financial Services	<ul style="list-style-type: none"> • Assistant Secretary of the Navy for Financial Management (FMO)
Logistics and Weapons Industrial Base	<ul style="list-style-type: none"> • Assistant Secretary of the Navy for Research, Development and Acquisition Director of Supply Programs and Policy (CNO N41) War Reserve Materiel and Readiness Branch (HQMC LPP-1)
Transportation	<ul style="list-style-type: none"> • Director of Supply Programs and Policy (CNO N41) Military Sealift Command
Space	<ul style="list-style-type: none"> • Space Systems Division (CNO N63) Navy Space Command
Defense Information Infrastructure/Command, Control, and Communications	<ul style="list-style-type: none"> • Director, Information Transfer Division (CNO N61) Deputy Assistant Commandant for Systems Integration (HQMC C4)
Intelligence, Surveillance, and Reconnaissance	<ul style="list-style-type: none"> • Director, Requirements, Plans, Policy and Programs Division (CNO N20) Intelligence Plans and Policy Branch (USMC I)
Public Works	<ul style="list-style-type: none"> • Assistant Secretary of the Navy for Installations and Environment Director, Ashore Readiness Division (CNO N46) Director, Facilities and Services Division (HQMC I&L (LF)) Naval Facilities Engineering Command

Figure 7.3-3—The DON CIP Working Group is comprised of subject matter experts supporting the CIP sector construct.

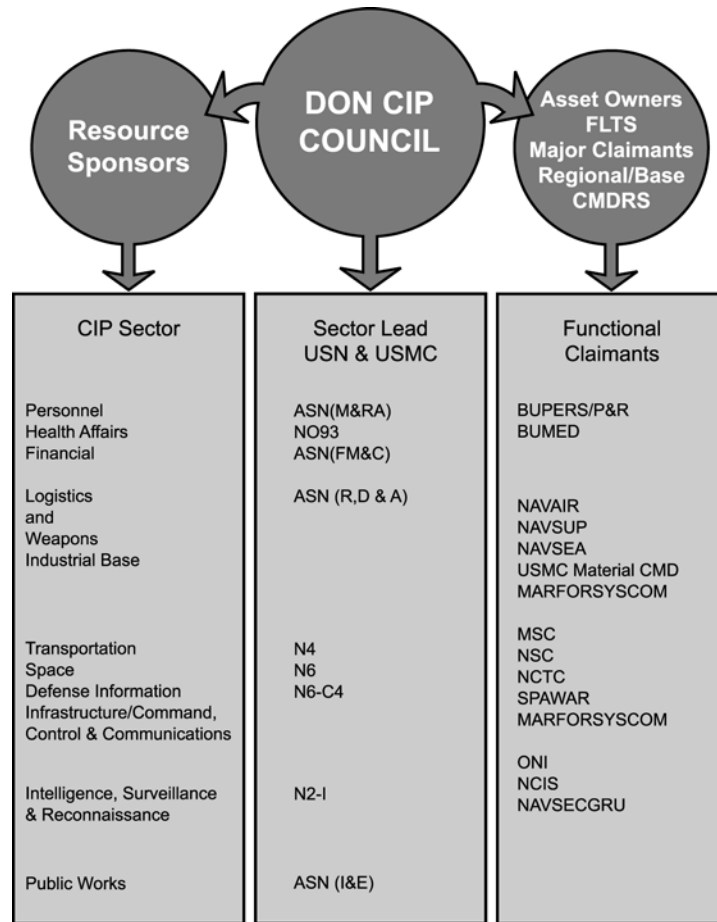


Figure 7.3-4—On the CIP Council, DON Sector leads represent the interests of their respective components for their particular infrastructures.

The DON CIP organization provides a common management environment within which CIP-related programs are planned, coordinated, integrated, and administered. The DON CIP organization assists the DoD sector CIAOs in the development of Defense Infrastructure Sector Assurance Plans by providing DON sector specific information and supporting the identification of inter and intra dependencies.

The DON CIP organization is composed of representatives of the Navy and Marine Corps, and special function providers, such as the NCIS for indications and warnings and inside the gate assessments, and JPO-STC for outside the gate assessments. The DON CIP organization serves as a forum for CIP issue coordination throughout the DON. As shown in Figure 7.3-4, the DON sector leads represent the interests of their respective components for their particular infrastructure. For example, the Navy Surgeon General (N093) represents the interests of the DON for the Health Affairs Sector.

CIP WORKING GROUP

Most of the CIP effort consist of decentralized execution. While most CIP objectives can be met through virtual collaboration, DON CIP organization members meet periodically for centralized planning and issue resolution. The functions of the DON CIP Working Group are defined in the following paragraphs.

Coordinate DON Implementation and Execution of the DoD CIP Plan. Due to the diversity of the Navy and Marine Corps assets within the DON and their relationship to their respective DoD sector, uniform DON execution of the DoD CIP Plan is unrealistic without a central coordinating entity. The DON CIP Working Group serves as the coordinating entity to leverage the knowledge and experiences of CIP across the DON to optimize the program benefits and ensure uniform execution in the interest of mission assurance.

Assist DoD Sector Leads and Special Functions in Development of Assurance Plans. Members of the DON CIP Working Group assist the DoD Sector Leads and Special Function components in development of their Assurance Plans (as required by the DoD CIP Plan).

Develop and Coordinate the Unified and Individual DON CIP Resource Plan(s). An objective of the DON CIP Working Group is to support DON resource sponsors and supporting organizations to identify funding requirements for executing CIP throughout the DON, and to invest in approved protective measures improvements, remediation, mitigation, and restoration activities. These funding actions can range from supporting initiatives within the DON Sectors, to the protection of assets that have been identified as critical to DoD/DON's force readiness and operational capabilities. Once the funding requirements associated with each of the protection activities have been identified, the DON CIP Working Group will prioritize these funding requirements and present them to the DON CIP Council for concurrence before submission for inclusion in the DoD CIP Resource Plan. The DON CIP Working Group will produce an annual DON CIP Resource Plan that provides a complete picture of the funding profiles and requirements of CIP-related activities in the DON. The DON CIP Council will review the DON CIP Resource Plan and recommend funding actions.

Facilitate Integrated Infrastructure Analysis, and Assessment, and Vulnerability Remediation throughout the DON Enterprise. A fundamental requirement of CIP is to understand the DON's reliance upon critical infrastructures. With this requirement in mind, analysis efforts focus on analyzing DoD/DON, National, and international infrastructures in the context of scenarios and operation plans (OPLANs) to identify critical assets. Once critical assets are identified, assessment efforts focus on identifying both physical and cyber vulnerabilities to those Department and commercial infrastructures that are critical to Military mission success. The DON CIP Working Group and Council then work with asset owners—whether DON, government, or commercial—to develop effective vulnerability mitigation efforts focusing on infrastructure protection investment strategies, operational protection enhancements, and contingency plans.

Facilitate an Integrated DON CIP Indications and Warning Capability. The DON CIP Indications and Warnings Lead and the DON CIP Working Group support DoD Intelligence, Surveillance and Reconnaissance (ISR) Sector Lead and Intelligence Special Function Component leads in identification of requirements and capabilities to develop indications and warning processes and procedures to ensure timely receipt and coordination of information.

Develop DON CIP Policy and Planning Documents. The DON CIP Working Group assists the DON CIAO in the development and dissemination of relevant, Enterprise-wide CIP policy and coordinates, with the Critical Infrastructure Protection Integration Staff (CIPIS) and Defense Infrastructure (DI) Sector Leads, to identify issues that require DoD policy clarification, and assists in the review and coordination of proposed DoD policy. The DON CIP Working Group develops appropriate sector and special function specific policy, planning, and implementation documents to ensure comprehensive integration of CIP throughout the DON.

Assist in Coordinating Interagency and National Level CIP Issues. Requests for support regarding National-level CIP initiatives are handled through the DON CIAO Office. The DON CIP Working Group assists the DON CIAO Office on national issues pertaining to Critical Infrastructure Protection that require coordination with outside organizations, both government and private sector.

Assuming proper funding, by FY 2003 the DON CIP program will have ushered in a paradigm shift in the management and evaluation of Navy and Marine Corps installations and weapon systems sustainment operations. Some of the more revolutionary products of DON CIP are implementation of the Naval Integrated Vulnerability Assessment process that encompasses Antiterrorism and Force Protection, Operational and Information Security, Mission Survivability, and “mission critical” non-organic infrastructures—in both “assigned team” and “self assessment” versions; and development of a DON Critical Infrastructure Vulnerability Database and Remediation Plan. The DON has developed a fully integrated counter intelligence information sharing construct, and quantified the value of each DON installation relative to warfighting operations. Policy for ensuring commercially provided weapon system sustainment operations is also being developed.

Being able to objectively rank the contribution to warfighting operations of installations and infrastructures will enable DON senior leadership to deal more effectively with issues such as base realignment and closure. We would not be surprised to see the conventional wisdom of the career enhancing value of shore based command evolve to “installation contribution to operating plan” from the current “installation size and population.”

Ultimately DON CIP would hope to be integrated into, and become a major contributor to, a national CIP network that optimizes the positive power of the Federal sector to protect the citizenry, institutions, and continuity of government operations.

WHAT DOES SUCCESS LOOK LIKE: A STORY

In the first year of the DoD CIP program the Department of the Navy volunteered to host the first ever combined Defense Integrated Vulnerability Assessment in the Pacific Northwest Region of the US. A major objective was to determine if investigative elements of the Joint Staff, a Military service, and independent monitors could work a “region,” collectively covering a number of bases as well as the commercial infrastructure servicing those bases. This type of cooperation was unprecedented.

Teams from the Defense Threat Reduction Agency, Naval Criminal Investigative Service, and Joint Program Office for Special Technology Countermeasures split up the region and went to work gathering data and conducting exercises. Cooperation was achieved—and vulnerable infrastructures identified.

The CIP construct was confirmed and its potential value proven. The DON takes great satisfaction with having been at the forefront of this groundbreaking, paradigm shattering, effort. Building on the success of this endeavor, the Department conducted an even more expanded Integrated Vulnerability Assessment effort in Southern California. Regional assessments will continue, on a rotating basis, to ensure all Naval regions are evaluated.



While this groundbreaking Naval Integrated Vulnerability Assessment process will provide great benefits to the Naval activities in our large regional concentrations, there are numerous other Naval activities that will not be included in these regional assessments. To ensure that all of our people and critical infrastructures are protected, the Department of the Navy has developed a *CIP Self Assessment Tool* CD, the first of its kind, that allows individual commands to identify vulnerabilities, both on-base and off-base, and develop risk mitigation strategies.

7.4 Privacy

Protecting an individual's private and personal information, both on the Internet and intranet, is an ethical responsibility of every organization.

—CAPT Mike Wendling, USNR, DON CIO Privacy Team Leader

BACKGROUND

Coming home one evening from a long day of work, you unlock your door and close it behind you feeling safe and protected from unwelcome intrusion. As you log on to your computer, you notice an e-mail from someone unknown to you. You open the e-mail to find the following message:

“The door to your system was unlocked, so I let myself in. Hi, how was work today at the ABC Company? I hope you get that raise you have been working so hard for. You will need it to qualify for that new car loan you applied for last week. By the way, you are going to look great in that new outfit you bought at the online XYZ Store. Based on your earlier chat session with John, I am sure he will really like it when you meet him tonight for your date.”

Shocked and dismayed, you quickly turn off your computer and wonder how such an act could have happened to you and what you need to do to make it stop. You quickly realize that your haphazard use of your social security number on the Internet could have compromised your personal identity.

Privacy protection is a key initiative of the Department of the Navy's Chief Information Officer (DON CIO). With increasing reliance on the Internet and electronic means to collect, store, and disseminate personal and sensitive information, the vulnerability of this information to unauthorized access and misuse is growing at Internet speed. In the effort to protect our critical knowledge assets, we must recognize the importance of protecting the individual. The increased importance of the individual as the “node on the network” means that increasing amounts of private and personal information become part of our information superiority. It is of vital importance that every effort be made to safeguard that information in the same fashion that we protect our forces.

With the rapid dissemination of sensitive information, such as home addresses and phone numbers, social security numbers, birth dates and even buyer preferences, consumers—and now the Federal Government—are growing more concerned with how that information is obtained and used. The issue of Internet privacy has begun to build up steam in Congress where several legislative initiatives are being debated. Public awareness and concern regarding the unauthorized collection and release of private/sensitive information demand that the DON and other Federal agencies take appropriate actions to inform and protect all users and ensure that any data collected or maintained by the agency is secure.

Why does this concern the DON? Information is a critical resource in DON operations and management. The proliferation and ease of use of computer technology have created an environment in which an individual, business, foreign government, or terrorist can easily access personal or private information on organizations and individuals. The DON must be able to protect the privacy of its personnel and operations, as well as that of other agencies and contractors.

FEDERAL REQUIREMENTS

The Federal Government considers the protection of personal privacy in today's digital age a top priority. The Privacy Act of 1974 requires Federal agencies to establish appropriate safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity. Throughout the 1990s, rapid advances in information technology (IT) allowed the Federal Government to offer an increasing number of electronic services to the public. The same technology that has improved efficiency and productivity of Federal agencies, however, has also created the need to reevaluate personal privacy issues.

In 1996, recognizing the importance of information technology for effective government, Congress and the President enacted the Clinger-Cohen Act, which requires the heads of Federal agencies to link IT investments to agency accomplishments. It also requires that agency heads establish a process to select, manage, and control IT investments. Privacy Impact Assessments (PIAs), which are methodical processes for addressing privacy issues as new systems are being developed, may become the prevalent model to ensure privacy as new IT systems are implemented. While privacy policies outline best practices and planning at a policy level, PIAs evaluate the level of privacy in information systems at all levels throughout the system life cycle, from design to deployment. Congress and the Office of Management and Budget (OMB) have recognized the Internal Revenue Service PIA, completed in 1996–97, as one of the best practices in government. The DON CIO is developing a PIA to address specific concerns of the DON.

The Privacy Act of 1974 directs the OMB to develop and prescribe appropriate guidelines and regulations to Federal agencies on the collection and maintenance of private information. With the birth of the Internet and subsequent concerns over the management of Federal information systems, OMB has, in the past several years, had an increased role in developing new guidance that responds to concerns not directly addressed by the Privacy Act of 1974.

In February 1996, the OMB issued circular A-130 on Management of Federal Information Resources, which requires Federal agencies to establish information management policies that respond to the privacy rights of individuals and “ensure that appropriate legal and technical safeguards are implemented.” In June 1999, OMB released the Memorandum (M-99-18), “Privacy Policies on Federal Web Sites,” which requires agencies to post clear privacy policies on principal Web sites, at other major entry points to sites, and at any Web page where substantial amounts of personal information are posted.

A year later, OMB released its Memorandum on “Privacy Policies and Data Collection on Federal Web sites” (M-00-13), reminding Federal agencies that they are required by law and policy to establish clear privacy policies for their Web activities. It also offered additional guidance with regard to Web technology that can track activities of users over time and across different Web sites. It states that “cookies,” which are small bits of software that can be placed on a Web user’s hard drive, should not be used at Federal Web sites, or by contractors when operating Web sites on behalf of agencies, unless, in addition to clear and conspicuous notice, the following conditions are met: a compelling need to gather the data on the site; appropriate and publicly disclosed privacy safeguards for handling of information derived from cookies; and personal approval by the head of the agency. In December 2000, OMB also issued guidance (Memorandum M-01-05) that required Federal agencies to incorporate measures to safeguard privacy concerns when sharing information.

In September 2000, the General Accounting Office (GAO) found that the overwhelming majority of Federal agencies reviewed adhere to OMB guidance. However, the GAO also determined that OMB guidance was vague and lacked necessary definitions regarding “major entry points” and “substantial personal information.”

DON AND PRIVACY

The Internet has become a powerful tool for transmitting and communicating information critical to the Department of the Navy. Operations, logistics, and the day-to-day management of DON affairs are heavily dependent on the protection and continued privacy of its information resources. These resources may include medical records, personnel data, deployment locations, new weapons acquisitions, and other critical information that must be protected.

However, such resources can become vulnerable by allowing sensitive or inappropriate information to be distributed openly or accessed via publicly available Web sites. As former Secretary of the Navy, Richard Danzig, warned in July 1999:

The global reach of the World Wide Web requires special precautions be taken when posting information to this medium...Recent advances in computer software and Internet-based search engines have given Web users the ability to automatically ‘mine’ data and collect an aggregate of information that can pose a threat to the security of Navy operations and the personal safety of Navy forces and their families.

Most publicized privacy information is vulnerable to illegal incursions into government systems by state and sub-state terrorist groups, professional criminals, hackers, or even fellow employees. Such information can be used to disrupt DON operations or endanger personnel, and the number of incidents that are reported is growing. The crime of “identity theft,” for instance, is a vulnerability of which the DON must be aware in order to protect its personnel.

Identity theft occurs when someone's credit or other personal information is obtained and used by another to obtain goods and services under the fraud victim's name. The amount of information needed to conduct such activities is relatively minimal; information found on a driver's license, credit card, social security card, and more sensitive information, contained within DON information systems, is vulnerable to misuse. DON personnel and other agencies must be assured that privacy policies exist to protect sensitive and personal information.

PRIVACY CHALLENGES

While the DON is working to secure the lines of communication and protect its infrastructure, there is a significant conflict between protection and privacy. According to the Electronic Privacy Information Center (EPIC), "the most recent dangers to civil liberties come from the new-found threat to our nation's infrastructure." While national guidance, such as Presidential Decision Directive 63 (PDD-63), instructs Federal agencies to develop thorough Critical Infrastructure Protection (CIP) and Information Assurance (IA) policies, concerns arise that the monitoring and controlling of the infrastructure and information systems may be used to erode the privacy of U.S. citizens. Law enforcement and prosecution tools (for example, the FBI's system formerly known as Carnivore) are also criticized for potentially violating the Fourth Amendment. Finally, many disagree with new categories of classification used to provide infrastructure protection and information assurance, such as "unclassified sensitive" and "aggregate sensitive." To privacy advocates, the increase in governmental secrecy is seen to be taking steps backwards.

Some privacy advocates, such as the group, Americans for Computer Privacy, assert that government must not mandate the choice of technology or dictate standards that violate personal and corporate privacy in the quest for CIP and IA. One specific tool used by the government that may be controversial to some privacy advocates is the banner warnings that appear when logging into DoD (and other) computers. Basically, these warnings state that use of the system implies consent to be monitored. Despite the fact that this warning is on government-owned work-related computers, some do not believe any monitoring of systems is appropriate. The banner, however, allows investigators to track down intruders and mitigate any damage done to the system.

Additionally, there is a conflict between privacy groups and security experts who wish to add a biometrics level to the defense-in-depth strategy. Essentially, a biometric measures a physical trait or personal characteristic of an individual and uses that to positively identify the individual. An example of a biometric measure is a fingerprint scan. To many IA and CIP experts, this layer is the ultimate in security and assurance. To privacy watchdogs, it is the ultimate invasion of privacy because personal minutiae are made vulnerable to identity theft. There are emerging technologies that will allow the biometric to be linked to an anonymous pin (rather than to an individual's name) and function much like Public Key Infrastructure (PKI). The DON CIO is exploring privacy concerning the use of biometrics.

Finally, there is a conflict between the Military's work on CIP and IA and *Posse Comitatus*. Essentially, the doctrine of *Posse Comitatus* states that the U.S. Military may not execute laws within the U.S. without an act of Congress. This brings into question the

ability and feasibility of the Military to monitor non-DoD systems, such as local energy companies, to protect the infrastructures to Continental United States bases and installations. In wake of the September 11 terror attacks against the United States, the DON will be challenged with striking a delicate balance between privacy and security.

IMPLEMENTATION

Building confidence in the protection and continued privacy of DON information must be a central focus of information assurance planning. Privacy, as an integral part of this effort, must include the development of privacy policies, training and education, technological tools and resources, and information collection safeguards.

Privacy Policy

In the most recent policy guidance pertaining to the Privacy Act of 1974, the Secretary of the Navy issued a privacy instruction (5211.5D) on July 17, 1992 that provides comprehensive policies and procedures for:

- Governing the collection, safeguarding, maintenance, use, access, amendment, and dissemination of personal information kept by DON in systems of records.
- Notifying individuals if any systems of records contain a record pertaining to them.
- Verifying the identity of individuals who request their records before the records are made available to them.
- Notifying the public of the existence and character of each system of records.
- Exempting systems of records from certain requirements of the Privacy Act.
- Governing the Privacy Act rules of conduct for DON personnel, who will be subject to criminal penalties for noncompliance with Federal policy.

Both the Privacy Act of 1974 and the SECNAVINST 5211.5D lack important guidance pertaining to the protection of personal information on new technologies such as the Internet. In response, the DON CIO, responsible for providing Department-wide information management and information technology leadership and guidance, is updating, developing, and implementing sound privacy policies and procedures for information management systems and technology.

Additionally, procedures are in place to address special precautions when posting DON information to the Web, determining appropriateness of information, identifying and securing sensitive information, establishing procedures to ensure continued privacy of information, and determining mechanisms for reviewing information. Privacy policies and procedures establish criteria for such measures as well as provide access controls. Additionally, privacy policies are to be widely disseminated and clearly understood by all DON personnel—both Military and Civilian. It will remain important that employees understand that there is only a limited expectation of privacy and that DON owned systems can, indeed, be monitored.

Training, Education, and Awareness



The establishment of a sound privacy policy furthers the DON's capability to address this issue. Understanding these policies, as well as the potential threat, by providing training and education throughout the Navy and Marine Corps is important. DON personnel must possess enough information to understand how and why sensitive information may be vulnerable to misuse, as well as what actions can help prevent such a situation. DON CIO has developed a privacy awareness CD that includes important privacy policies and procedures for all DON personnel. The publication will also include specific information on how individuals can protect themselves from the growing risk of identity theft. Updated versions of this tool will be continually released as the Federal privacy environment changes. Confidence building through training, education, and awareness is essential to appropriate privacy policy compliance.

Technological Tools and Resources

Technological tools and resources are also available to protect information. The private sector has capitalized on the consumer demand for such tools. The Senate Judiciary Committee's recent publication, *Know The Rules, Use The Tools, Privacy in the Digital Age: A Resource for Internet Users*, outlines a number of resources to protect personal information, including identity scrubbers, privacy preferences, digital identity managers, encryption, and cookie controls. In addition to such tools, DON must utilize technologies to regularly monitor Web sites and information systems for vulnerabilities and possible incursions. Publicly accessible material, in particular, must undergo screening for appropriateness. The use of password protection for sensitive information is also critical.

Collection and Safeguarding of Information and Data

With increasing sensitivity over ensuring privacy, it is also worth emphasizing that DON privacy policies will include procedures and criteria for collecting information from public users. Currently, DON CIO is working closely with the Naval Audit Service (NAS) and the Navy's Chief of Information (CHINFO) to ensure that DON components follow strict privacy guidelines for information collection and dissemination on Web sites and information systems.

LOOKING FORWARD

In response to Federal guidelines, DON CIO has chosen privacy as one of its key initiatives to address throughout the next several years. While DON will continue to comply with new or amended privacy guidance or legislation, what sets DON apart from most other actors in today's privacy environment is its foresight to embrace strong privacy practices before its personnel demand them. DON CIO has taken proactive measures to make its personnel aware of their privacy rights and guidelines through measures such as education and awareness CDs, training presentations, and privacy surveys. The success of these initiatives is evident in the positive response from DON offices and enthusiastic

adoption of privacy best practices throughout the DON. In more concrete terms, success can be measured in the scope and offerings of the DON CIO Privacy Team. What was begun as an operation to assure privacy compliance has evolved to a fundamental theme in the DON CIO's mission.

DON CIO is working diligently to ensure that the Department's Web sites are in compliance with current OMB, DoD, and other regulations or policies. In order to do so, DON CIO has asked the National Audit Service to audit Web sites for cookies, privacy statements, and Web bugs. Additionally, Congress directed Federal agencies to conduct an audit of privacy practices and policies which the DoD Inspector General's Office (DoD IG) has been directed to complete. With each audit, several of DONs physical sites will be evaluated for privacy policy and procedure compliance. The DON CIO is developing a privacy policy and a Web based Privacy Impact Assessment, which are expected to be released in the fourth quarter of fiscal year 2002. The PIA will serve as a privacy risk management tool used during major system development or modification cycles.

CONCLUDING THOUGHTS



As the Department of the Navy endeavors to secure the pathways of knowledge, while respecting the right to privacy of its workers, it is faced with challenges, such as new technologies, that change the way in which personal information must be kept secure. It is imperative that policy decisions keep pace with the technology that drives them. Because of the integrated nature of the DON CIO team, the security policies established for the DON reflect the importance of privacy while maintaining the security needed to ensure the protection and performance of the warfighter. The DON is sensitive to the right to privacy of its Military and Civilian members. Hence, each security measure is fully vetted to ensure it meets the privacy regulations of the Federal Government, DoD, and DON, while complying with the overall Federal IA and CIP missions.

CHAPTER 8

Focus On Dollars

- 8.1 *The IT Capital Planning Process*
- 8.2 *Investment Management*
- 8.3 *Enterprise Licensing*
- 8.4 *Metrics*

INTRODUCTION

Effective information technology (IT) capital planning cannot occur without linkage to the Department of the Navy (DON) Information Management/Information Technology (IM/IT) Strategic Plan. Because of this inter-relationship, IM/IT strategic planning is considered the foundation or necessary first step to effective capital planning. The IM/IT Strategic Plan defines the DON IM/IT vision, guiding principles, mission, goals, and objectives and, in so doing, provides the basis for the development of annual Navy and Marine Corps IM/IT investment strategies to support the Department's missions and objectives. The IM/IT investment strategies, in turn, serve as the driver of IT capital planning. During the selection or funding approval phase of the capital planning process, the specific IM/IT investments that satisfy the minimum decision criteria for funding, and that support the approved investment strategies, are the investments which are approved for funding during Program Objective Memorandum (POM) or budget formulation, or during budget execution.

Investment strategies provide the roadmap for allocation of resources to achieve the goals and objectives contained in the DON IM/IT Strategic Plan. In the investment strategies step, planners identify alternative approaches to achieve these objectives, rate them in terms of their estimated effectiveness in achieving a particular objective, and select a strategy or set of strategies that will best achieve the level of performance specified for that objective in the Strategic Plan. Navy and Marine Corps managers then are able to evaluate individual investment alternatives against the strategies to ascertain if the investments facilitate achievement of those strategies as a prerequisite for funding approval. A key step in achieving objectives is Investment Management. Investment Management is a process that helps Navy and Marine Corps decision-makers maximize the value and manage risk associated with IT investments.

Enterprise Licensing supports the organization's ability to program, budget, acquire and manage its software assets in a number of critical areas. First, Enterprise Licensing ensures effective alignment of the software asset to the organization's mission and strategic goals. This is done in the Portfolio Management process by ensuring that the IT investment is linked directly to the organization mission through the Enterprise license. Enterprise Licensing also permits decision-makers to view a particular software investment from an Enterprise perspective, and to identify investments that are interdependent. Overbuying of licenses can then be avoided and opportunities for resource sharing and reuse can be identified.

Second, Enterprise Licensing can serve as the common thread linking all phases of capital planning: selection, management, and evaluation. It does this by consolidating the resources and related investments that are required to accomplish a mission-related or administrative outcome under the Enterprise license. Tracking of the asset status is improved and measurable improvements to mission outcomes can be achieved.

Third, Enterprise Licensing permits collection of historical data on the software asset that can be used to improve the Software Asset Management process. The focus of Software Asset Management is on tracking and managing the software license. This approach permits identifying and managing the associated asset attributes such as cost, version, terms and conditions, and maintenance agreement information. A Software Asset Management Framework is used to capture and integrate the physical, financial, and contractual data to support and optimize the management functions that are necessary for effectively managing and optimizing a software portfolio.

Finally, Enterprise Licensing is flexible enough to be used at any level of the organization. Senior managers with the programmatic responsibility in key business areas can use Enterprise Licensing directly in prioritizing, selecting, and managing their subset of the Enterprise software portfolio. Decisions made related to these investments are based on strongly-aligned goals and objectives, and quantifiable data identified directly to the Enterprise License. A mature Enterprise Licensing process is a continuous activity, and not just a process to be done at budget and procurement time.



INSIGHT

In the culture of the Department of the Navy metrics are critical for success. What we have learned along the way is to create metrics that measure the desired future rather than the past.

Metrics, or performance measurement, is a key component of effective management. Performance measures are the standards used to measure success in achieving an objective. Performance measures describe the precise measurement that will generate a quantitative (or qualitative) indicator that explicitly or implicitly indicates progress towards achieving the objective. The Government Performance and Results Act of 1993 directs that agencies report performance through measures that relate to their strategic goals. The Clinger-Cohen Act of 1996 further directs that agencies manage IT using performance measures that measure how well the IT supports their missions.

Performance measures are used to support the selection, funding, acquisition, deployment, maintenance, and enhancement of an investment. Focusing on dollars, performance measures are developed during all phases of IT Capital Planning. In this chapter, performance measures are discussed for IT in general and for knowledge management initiatives specifically.

8.1 The IT Capital Planning Process

Results that are not measurable don't count.

—Carl E. Bolter, Director of Resource Management

BACKGROUND

Increased public scrutiny, tighter budgets, and legislative mandates all compel information technology (IT) managers to focus their attention on managing IT investments, rather than focusing too narrowly on IT acquisitions. The emphasis must be on achieving outcomes that contribute to mission effectiveness. To achieve success, a systematic capital planning approach for IT investments is needed to manage the risks and measure the benefits in support of a given mission.

As depicted in Figure 8.1-1, the three phases of the capital planning process occur in a continuous cycle of selection, management, and evaluation. Information from each phase flows freely among all of the phases. The flow of information from the evaluation phase to the selection phase reflects the potential modification of selection phase funding decision criteria resulting from post-deployment reviews. Similarly, the interchange between the management and evaluation phases reflects the exchange of milestone review decision information and potential modifications to approval criteria.

Capital planning is an integrated management process which provides for the selection, management, and evaluation of IT investments over their life cycles.

Capital planning requires discipline, rigor, executive management involvement, accountability, and focus on risks and quantified benefits. Actual benefits, when compared to projected benefits, are used to measure an IT investment's relative success or failure. The overall objective of a structured capital planning process is to fund those IT investments which deliver the greatest business benefit to the Department of the Navy (DON). More specific objectives are:

- Facilitate achievement of DON IT investment strategies which support goals and objectives in the DON Information Management/Information Technology (IM/IT) Strategic Plan.
- Facilitate achievement of DON's mission and business objectives.
- Maximize benefits while minimizing costs and risk.
- Measure performance and net benefit for dollars invested.
- Provide continuous feedback to help senior managers make decisions on new or ongoing investments.
- Ensure that public funds are spent responsibly.

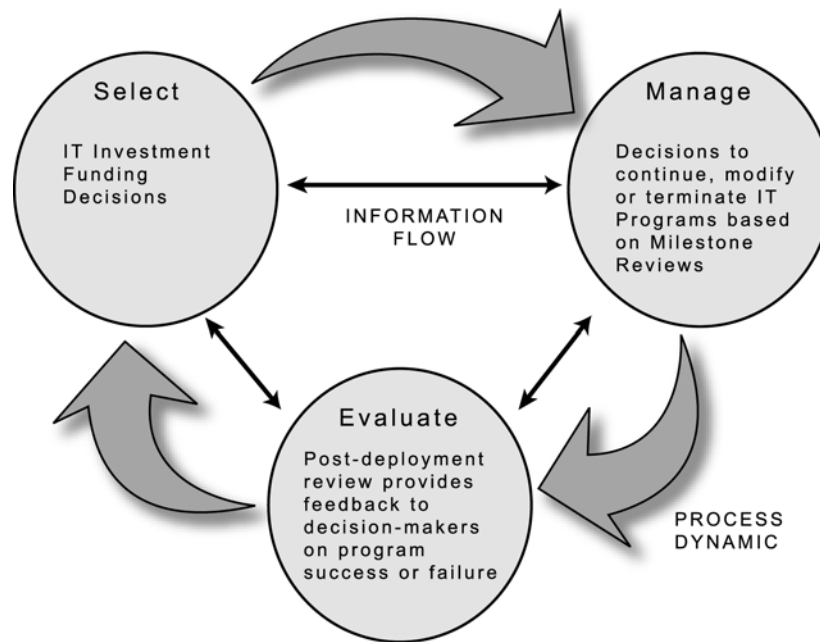


Figure 8.1-1—The capital planning process is a continuous cycle of selection, management, and evaluation.

Overall, capital planning uses long-range planning and existing, institutionalized processes for selecting and managing the portfolio of IT capital assets to achieve performance improvements at the lowest total ownership costs and least risk. These processes provide management with accurate information on acquisition and life cycle costs, schedules, and performance of current and proposed capital assets. This information will help in decision-making regarding the best use of available funds to achieve strategic goals and objectives.

CLINGER-COHEN REQUIREMENTS

The Clinger-Cohen Act (CCA) of 1996, Section 5122, requires that the head of the agency implement an IT investment capital planning process which:

- Provides for the selection, management, and evaluation of IT investments.
- Is integrated with the processes for making budget, financial, and program management decisions.
- Provides the means for agency management personnel to obtain timely information regarding the progress of the IT investment including the status of meeting specified milestones in terms of cost, schedule, quality, etc.
- Bases IT investment funding decisions on minimum criteria which facilitate the comparison and prioritization of competing IT investment alternatives.
- Provides for the identification of investments with potential benefits to other governmental agencies.

- Provides for the identification of measurements which quantify the risks and benefits of the investment to the mission or business area.

In 1997, the Secretary of the Navy (SECNAV) informed the Office of Management and Budget (OMB), who was assigned CCA compliance oversight responsibility by Congress, that the DON would use the existing Planning, Programming and Budgeting System (PPBS) and Acquisition processes to select, manage, and evaluate IT investments rather than create a duplicate capital planning process for those investments. The decision to use these existing, institutionalized processes ensured that IT investments would be subjected to the same management considerations as all other investments, i.e., that they would be selected for funding based on contribution to mission accomplishment and relative benefits and risk; and monitored and evaluated for progress and outcome/output periodically and routinely over their life cycles.

The decision to implement the IT capital planning requirement through the existing Planning, Programming and Budgeting System (PPBS) and Acquisition processes meant that there would be no separate IT capital planning process within the DON. Therefore, the policies and procedures governing the PPBS and Acquisition processes would also govern the selection, management, and evaluation of IT investments. An immediate benefit associated with designating the PPBS and Acquisition processes as the IT capital planning process solution was that it satisfied the CCA requirement to:

- Provide a process for the selection, management, and evaluation of IT investments.
- Establish a process that was integrated with the processes for making budget, financial, and program management decisions.
- Provide the means for agency management personnel to obtain timely information regarding the progress of the IT investment including the status of meeting specified milestones in terms of cost, schedule, quality, etc.

The decision to use the institutionalized PPBS and Acquisition processes for IT capital planning also recognized that IT investment funding and management decisions were ultimately the Secretary's, as mandated by the law, and not the Chief Information Officer's (CIO's). Another benefit associated with this decision was that it mainstreamed IT investment funding and acquisition/management decisions by placing those decisions in the hands of PPBS and Acquisition officials who routinely make those same decisions for all investments based on priorities, relevance to mission or business area goals or objectives, benefits, and affordability.

The decision to designate the PPBS and Acquisition processes as the IT capital planning solution did not in-and-of-itself completely satisfy the requirements of Section 5122 of the CCA. Policies still had to be established to satisfy the following requirements of Section 5122; specifically, to:

- Base IT investment funding decisions on minimum criteria which facilitate the comparison and prioritization of competing IT investment alternatives.
- Provide for the identification of investments with potential benefits to other governmental agencies.
- Provide for the identification of measurements which quantify the risks and benefits of the investment to the mission or business area.



While not the process owner for either the PPBS or the Acquisition process, the DON CIO took the initiative to formulate proposed policy for the Department regarding minimum decision criteria for funding approval to meet the requirements of Section 5122 described above. That proposed policy, discussed in greater detail in the “Selection Phase” section which follows, was staffed with the DON PPBS process owner (i.e., DON Program Information Center (PIC)) before formal dissemination within the Department. The DON CIO also successfully lobbied for formal inclusion in the PPBS and Acquisition decision-making processes by being designated an official member of the SECNAV-chaired DON Program Strategy Board, the senior DON decision-making body on financial issues, and a principal advisor to the DON acquisition official Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RD&A)) on all major IT acquisition programs.

Following is a discussion of the policies and procedures which govern the selection, management, and evaluation phases of the DON IT capital planning process.

SELECTION PHASE

During the selection phase of the capital planning process, the benefits, costs, relevancy to mission and risks of all projects are analyzed and assessed for purposes of making funding decisions. Each project is supported by the equivalent of a business case which, at a minimum, addresses the minimum selection decision criteria discussed below. The business case identifies the organizational needs that the project is meeting or proposes to meet and provides information on the benefits, costs, and risks of the project. The information in the business case is continuously updated to ensure that it reflects the current situation. After each project's costs, risks, and benefits are examined and validated, the funding sponsor or claimant compares all of the projects against common decision criteria in order to weigh the relative merits of the projects against one another and against other investment alternatives. As is the case with all investments, the actual decision to fund an IT investment in the final analysis is a function of affordability and the relative importance of the IT initiative to mission accomplishment, compared to other investments.

The selection phase takes place during the PPBS process. This is the phase of capital planning when actual investment funding decisions are made. In the DON, this may occur during the programming or POM development phase of PPBS, when decisions related to policy implementation, program levels, program direction, and affordability are addressed, or during budget development or execution. Following are discussions of the Navy and the Marine Corps planning and programming phases of PPBS, with focus on the IT investment funding decision-making process. Separate discussions for Navy and Marine Corps are provided due to differences in the Services' planning and programming processes. Also provided is a discussion of the DON budget process, which is identical for both the Navy and Marine Corps.

Planning, Programming and Budgeting System (PPBS) Process

Responsibility for planning and programming are delegated to the two separate Naval Services, Navy and Marine Corps, with staff offices consolidating a Departmental product for SECNAV who is the final decision-maker. In the planning phase of PPBS, the DON Office of Program Appraisal coordinates the work of the two Services' planning offices (the two Deputy Chiefs of Naval Operations for Plans, Policy and Operations (N3/5) and the Marine Corps Plans Division). These offices work with the Office of the Secretary of Defense (OSD) and Joint Chiefs of Staff planning staffs during preparation and review of draft Defense Planning Guidance. Program planning and preparation of the two Services' Program Objective Memorandum (POM) submissions are conducted separately by the Chief of Naval Operations (CNO), General Planning and Programming Division (N80), and the Marine Corps Deputy Chief of Staff, Programs and Resources (P&R), with a combined DON POM submitted to OSD by the DONPIC. The DON budget formulation process commences upon completion of the POM and is the responsibility of SECNAV.

Navy and Marine Corps Planning



The foundation of DON warfare assessment is the Integrated Warfare Architecture (IWAR) process. Multi-disciplinary Integrated Product Teams composed of members of the Navy, Marine Corps, and the Secretariat meet regularly throughout the year, independent of the PPBS process to conduct end-to-end capabilities-based analyses of the Navy's core investment areas, including Air and Sea Dominance, Power Projection, Deterrence, Information Superiority, Sustainment, Infrastructure, Manpower, Readiness, Training and Education, Technology, and Force Structure. The IWARs analyze issues such as relative contribution, criticality, cost versus benefits, synchronization, and sustainability with respect to specific capability investments. The analyses are shaped by policy and planning guidance, such as the Quadrennial Defense Review, Defense Planning Guidance, the CNO's Long Range Planning Objectives, Congressional actions, etc., and form the basis for the DON's near, mid, and long-term investment strategy.

The principal products of the IWAR process are description documents that feed development of the CNO's Program Analysis Memorandum (CPAM). The CPAM is a decision document constructed following detailed analyses of the IWARs and is intended to produce a balanced investment recommendation to the Department's senior leadership across all DON warfare capability areas. It includes not only detailed health assessments of the DON's core warfighting and support capabilities but also specific investment and trade-off recommendations. The CPAM also provides the bases for the programming guidance forwarded to resource sponsors each year early in the programming cycle. The outcome of the above Departmental planning process, along with OSD IM/IT Strategic Planning guidance, serves as the basis for the development of the goals, objectives, strategies, and initiatives reflected in the annual DON IM/IT Strategic Plan.

Summaries of the IWARs and CPAM are briefed to the Integrated Resources and Requirements Review Board (IR3B) and the DON Program Strategy Board (DPSB) each year. The IR3B is the focal point of the DON assessment process. In the planning phase, it reviews recommendations of the IWARs/CPAM and makes programmatic recommendations for POM development. The DON Program Strategy Board, chaired by SECNAV, resolves policy issues and reviews programs at the top level of DON management during the PPBS process.

Navy Programming

The Navy programming cycle commences with issuance of Preliminary Program Guidance, which documents initial investment guidance for Navy programs based on results of DON IWARs, the CPAM and the DON Programming Guidance issued by the SECNAV. Upon receipt of this guidance, Navy Resource Sponsors adjust their programs to meet fiscal and programmatic direction. This is also the Sponsor's opportunity to make technical corrections, fact-of-life cost adjustments, and other zero-sum changes within the bounds of the fiscal guidance to reflect program changes. The product of this process is the Sponsor Program Proposal which is the translation of planning guidance into specific Resource Sponsor programs and program levels. Sponsor Program Proposals and the proposed Navy program are reviewed and approved by the CNO before final approval by SECNAV.

Navy Resource Sponsors review IT investments under their cognizance which surface during POM development to ensure that IT investment funding decisions are consistent with the annual IM/IT investment strategy and are based on measures which quantify the benefits to their respective mission, business, or functional area. Minimum criteria examined as a prerequisite for funding approval are: (1) either quantified savings and/or cost avoidances (supported by Return-on-Investment and/or Net Present Value computations) or measures which quantify the performance improvements which will result from the investment; (2) relationship to DON mission or business area goals and objectives; and (3) risk.

An example of an investment criteria-ranking scorecard can be found in the DON IT Investment Portfolio Model, which is available electronically on the DON CIO Web site at www.don-imit.navy.mil. The IT Investment Portfolio Model is a tool which incorporates the above minimum criteria and other criteria pertinent to the decision-making process and which can be used at any organizational level to prioritize competing IT investment alternatives. The IT Investment Portfolio Model is discussed in greater detail at the conclusion of this chapter.

In reviewing IT investments for potential funding, Navy Resource Sponsors are able to evaluate the benefits and risk to their mission or business areas and the relationship of the investment to overall mission goals/objectives. For this reason and because IT is not a program but rather a support function or utility, a Navy-wide review of IT investments which would seek to prioritize investments between Sponsors is not considered appropriate.

A particular Resource Sponsor's overall investment portfolio reflects his/her evaluation of the IT investments required to fulfill his/her mission and business area goals in accordance with direction from the assessment process, the CPAM and DON Programming Guidance.

Marine Corps Programming

Programming in the Marine Corps differs somewhat from the Navy's process. The Marine Corps reviews POM proposals concerning operations, personnel, material, and systems by unique Marine Corps mission areas. Coordinated by the Deputy Chief of Staff, Plans and Resources, the Marine Corps POM submission is developed by the POM Working Group and reviewed by the Marine Corps Program Review Group. The POM Working Group is responsible for prioritizing and recommending funding profiles for all requested programs within the Marine Corps POM. After review of the POM Working Group's recommendations by the Program Review Group, proposals are forwarded to the Assistant Commandant's Executive Steering Committee for final program review. Following this review, the draft Marine Corps POM submission is forwarded to the Commandant of the Marine Corps for final approval prior to submission to SECNAV.

All Marine Corps IT program requests are centrally managed by Commander, Marine Corps Systems Command, as directed in policy from the Assistant Chief of Staff, Command, Control, Communications, Computers and Intelligence. Each IT investment funding request is prioritized on its own merit and benefit to the Marine Corps and, as is the case with all other investments, forwarded to the Program Review Group by the POM Working Group and to the Executive Steering Committee for endorsement to the Commandant. IT investments are reviewed by the Marine Corps against the same minimum decision criteria used by the Navy as a prerequisite for funding approval.

At the conclusion of the Navy and Marine Corps programming cycles, Tab G, which is the IT extract of the POM submission, is prepared by both the Navy and Marine Corps and is forwarded to Office of the Under Secretary of Defense (Comptroller) (Program Analysis and Evaluation) by the DONPIC. Tab G reflects the approved IT investment portfolio for both the Navy and Marine Corps as of the POM submission (i.e., the IT investment decisions resulting from the DON assessment and Navy and Marine Corps POM development processes).

DON Budget Formulation/Execution

In the DON, preparation of budget estimates begins after completion of Navy and Marine Corps POM development and submission to OSD. For the DON, the budget cycle consists of four phases. The first is submission of budget estimates by budget submitting offices to Office of the Assistant Secretary of the Navy (Financial Management and Comptroller) (Office of Budget and Fiscal Management) (OASN FM&C) (FMB). The budget submitting offices' budget submissions (including the IT/National Security Systems budget exhibits) to FMB reflect the IT investment funding decisions made by the budget submitting offices based on application of the minimum decision criteria during their

respective budget formulation processes. The transformation of program estimates into budget quality estimates occurs in the budget submission to FMB and the subsequent DON budget review. Whereas Navy and Marine Corps POM development focuses on affordability, policy implementation, and program levels, the internal DON budget review focuses on whether programs are properly priced, properly balanced, and executable. During this phase of the budget process, FMB likewise reviews IT investments with assistance by the DON CIO.

The second, third and final phases of the budget process are, respectively, the submission of budget estimates to OSD and OMB for review and final approval by the Secretary of Defense and the President; the submission of budget estimates from the President to Congress for review and approval by Congress; and the enactment of appropriations and execution of those appropriations by the DON.

The IT budget exhibits submitted to higher authority with the Department's budget submission during each successive phase of the budget process reflects the DON IT investment portfolio approved by the preceding phase's budget reviewing authority. Justification for each of the major IT investments is documented in Exhibit 300B in accordance with guidance contained in the DoD Financial Management Regulation.

The requirement to base IT investment funding decisions on the specified minimum decision criteria applies not only to budgeted IT investments but also to those investments which surface during execution. Decisions to fund these emergent requirements during execution must be supported by documentation addressing the minimum criteria as the basis for funding approval.

MANAGEMENT PHASE

Achieving maximum benefits from a project while minimizing risks requires that the project be periodically and consistently monitored and managed for successful results. During the management phase of the capital planning process, acquisition management officials are actively engaged in making decisions and taking actions to change the course of a project when necessary; and providing feedback to PPBS decision-makers (i.e., into the selection process), if applicable, for purposes of reflecting the appropriate changes in the funding availability/profile for a particular investment.

The management phase is characterized by decisions to continue, modify or terminate a program, based on reviews at key milestones during the program's life cycle. The focus of these reviews changes and expands as the investments move from initial concept or design and pilot through full implementation and as projected investment costs and benefits change. The reviews do not focus exclusively on cost and schedule concerns but also on ensuring that projected benefits are being realized, that risks are being minimized and managed, and that the project continues to meet strategic needs.

Whereas IT investment funding decisions made annually during the selection phase tend to occur only during the PPBS windows established for that purpose, information in the management phase is continuously collected, updated, and fed to Departmental

decision-makers. Management phase data consist of such items as comparisons of actual results achieved versus projections, and assessment of actual benefits from project pilots or prototypes. Cost, benefit, schedule, and risk information that was included in the business case, including the various analyses that were done to justify the investment, are updated as project implementation continues. Updates include any revisions to the justification necessitated by adding functional requirements.

As each project is reviewed at various stages during its life cycle, decisions are made regarding the future of the project. These decisions are unique for each project and are based on the merits of the particular program. Decisions may be made which call for the suspension of funding or make future funding releases conditional on corrective actions being taken. These situations are communicated to appropriate DON PPBS decision-makers for implementation during POM or budget development or budget execution.

A discussion of the Department of Defense (DoD)/DON acquisition process, as it relates to the life cycle management of IT programs, follows.

DON Acquisition Process for IT Investments

The existing, institutionalized acquisition program management process is the process used by the DON to manage IT investments throughout their life cycles. The DON acquisition process for IT investments is governed by: (1) DoD Directive 5000.1, "The Defense Acquisition System" of October 2000; (2) DoD Instruction 5000.2, "Operation of the Defense Acquisition System" of January 2001; (3) DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs" of January 2001; and (4) SECNAVINST 5000.2B of December 1996.

Both DoD 5000 series acquisition policy and SECNAVINST 5000.2B, "Implementation of Mandatory Procedures for Major and Non-Major Defense Acquisition Programs and Major and Non-Major Information Technology Acquisition Programs," establish a general model for managing major defense acquisition programs and major automated information systems but do not require that the entire process described therein be followed for each program. The model has been designed to allow flexibility in management in recognition of individual differences in major acquisition programs, provided fundamental tenets (e.g., minimize risk, maximize affordability) are observed. Similarly, program managers and Milestone Decision Authorities (MDA's) for non-major acquisition programs are expected to adhere to the process described in DoD 5000 series and SECNAVINST 5000.2B but may tailor the process, as appropriate, to match the characteristics of the non-major programs.

In the DON, a MDA conducts milestone reviews for all IT acquisition programs. For MAIS programs, DON program managers brief ASN RD&A to coordinate a DON position and prepare ASN RD&A for the OSD milestone reviews. The Program Decision Meeting process is used to conduct the program briefing. It is done concurrently with the OSD overarching Integrated Product Team to prepare for presentation to the OSD Milestone Decision Authority.

DON MAIS programs each have an established acquisition coordination team (ACT), co-chaired by the applicable Deputy Assistant Secretary of the Navy (DASN) and program manager. An ACT is a team of stakeholders from the acquisition, requirements generation, test and evaluation, and PPBS communities who represent the principal advisors to the MDA. For MAIS programs, the Program Decision Meeting is the ASN RD&A milestone review forum. Programmatic issues and status of the program are fully addressed and presented at the milestone review via a Program Decision Brief. The Program Decision Brief documents the status of the program at a specific time and is part of the official program decision record.

The DON CIO participates on the ACTs for MAIS programs and serves as one of the Program Decision Principal Advisors to ASN RD&A for all MAIS programs. In those capacities, the DON CIO attends all major IT acquisition program briefings and milestone reviews. It is through the ACT and in the role of Program Decision Principal Advisor that the DON CIO exercises his/her responsibility under Section 1 of Executive Order 13011. This responsibility includes monitoring and evaluating major IT programs based on performance measurements and recommending the continuation, modification, or termination of those programs based on the reviews.

Software Management

Acquisition policy requires that a MAIS acquisition strategy describe the planned use of independent expert reviews for all software-intensive programs.

Program managers for software-intensive MAIS's must: (1) use best processes and practices known to reduce cost, schedule, and performance risks; (2) plan a spiral development process for both evolutionary and single-step-to-full-capability acquisition strategies; and (3) fully consider software security requirements.

Commercial Off-the-Shelf Considerations

Acquisition policy requires that the program manager apply commercial item best practices and ensure that the MAIS co-evolves with reengineered business processes.

EVALUATION PHASE

The evaluation phase takes place after the project is delivered to the user and is operational. It closes the loop on the IT investment management process by comparing post-deployment actual benefits against estimates in order to assess performance and identify areas where future decision-making can be improved. Lessons learned during the evaluation phase are geared towards implementing future process improvements. Central to this process is the post-deployment review (PDR) with its evaluation of the historical record of the project. Once a project has reached a final end-point (e.g., the project is fully implemented or the project has been canceled), a PDR is conducted. This review usually occurs about 3 to 12 months after a project is fully operational and is conducted by a group other than the project development team to ensure that it is conducted independently and objectively.

The information gained from PDRs is critical for improving how the organization selects, manages, and uses its IT resources. Each PDR has a dual focus. It: (1) provides an assessment of the implemented project, including an evaluation of the development process; and (2) indicates the extent to which the Department's investment decision-making processes sustain or improve the success rate of IT projects. There are three essential areas that are evaluated as part of a complete PDR.

First, customer surveys are conducted to determine users' satisfaction with the end product. There is also a focused look at how well the project supports specific business processes. Many of the intangible benefits that were identified at the outset will relate to how customers and end users feel about the final project.

Second, a close look is taken to determine whether the implemented system has achieved its intended benefits, based on the baseline review made prior to initiation of the project, and whether this impact is still aligned with mission goals. An assessment is also made of other project-specific aspects, such as an estimate of cost savings that have been achieved, compliance with the Information Technology architecture, evaluations of the information product (accuracy, timeliness, adequacy, and appropriateness of information), and identification of additional maintenance or security issues.

Third, an evaluation is made of the technical aspects of the project, both current and future. This evaluation may focus on such factors as the competency of the workforce to use the new system and employee satisfaction or retention, the extent to which advanced technology was used, and the methodological expertise of the development team.

Information gathered during the evaluation phase is aggregated and fed back to management decision-makers, i.e., the MDA and program manager. The primary focus of the PDR is on evaluating a project's actual results compared to estimates generated during the various phases and milestone reviews of acquisition process (i.e., management phase) in terms of cost, schedule, performance, and mission improvement outcomes for the primary purpose of determining the causes of major differences between planned and end results. A secondary objective of the PDR is to identify any inappropriate systems development and/or program management practices and management phase approval criteria that need to be modified to ensure future IT program success.

In that regard, the PDR should provide a wide range of information regarding both the project and the process for developing and implementing the project. Specific information includes:

- An assessment of the project's effectiveness in meeting the original objectives.
- An identification of benefits that have been achieved, an assessment of whether they match projected benefits, and a determination of reasons for any discrepancies.
- An evaluation of whether original business assumptions used to justify the project were valid.
- A comparison of actual costs incurred against projected costs.
- A determination of how well the project met time schedules and implementation dates.

- Management and user perspectives on the project.
- An evaluation of issues that still require attention.

Outputs of the PDR include user evaluations of the effectiveness of the project, actual costs, measurements used to calculate benefits, a matrix comparing actuals to estimates, and documentation of business improvement assumptions used to justify the project. A number of key decisions are made during the evaluation phase, including an assessment of how well the project met its intended objectives, a determination of what changes or modifications



to the project are still needed, and if warranted, an identification of ways to modify or improve the overall investment management process to better maximize results and minimize risks. The results and recommendations that arise out of the PDRs combined with other project information are a critical input for senior decision-makers to use to assess the project's impact on mission performance. ✓

CONCLUDING THOUGHTS

A Capital Planning Guide was developed early in the DON CIO change strategy. The capital planning process will not remain static but will evolve and change over time as the Department learns more about what has been successful and what still needs to be improved. Potential modifications that may be made to the process include:

- Changing the management phase milestone decision criteria used for monitoring the progress of projects.
- Modifying the timeframes for reviewing projects during the management phase.
- Modifying the PDR methodology.

The results from one project will not provide enough information to allow significant modification to be made to the agency's IT decision-making processes. However, significant recurring system development problems found across multiple projects over time are cause for refining or even significantly revising the decision-making processes and criteria.

8.2 Investment Management

Investment Management helps decision-makers make better informed decisions at a time when they must do more with less.

—Joeneicy Lewis, Planning and Measurement Team Leader

BACKGROUND

In recent years, Congress has passed legislation that requires Federal agencies to examine and change their current operation and management practices in order to improve performance and achieve greater mission outcomes. The Department of the Navy (DON) Information Technology (IT) Capital Planning Guide identifies this legislation and further describes what organizations in the DON need to do to manage and acquire IT.

In support of Investment Management, the office of the DON Chief Information Officer (CIO) has developed the following products:

- *IT Investment Portfolio Management Guide*
- *IT Investment Evaluation Handbook*
- *Guide for Developing and Using IT Performance Measurements*

IT INVESTMENT PORTFOLIO MANAGEMENT GUIDE



In order to achieve the Department of Defense (DoD) goal of information superiority in support of the warfighter and decision-makers, the DON must field interoperable information capabilities. This guide provides an investment decision process that can assist in achieving information superiority. It supports the DON IT Capital Planning Process and focuses on IT Investment Portfolio Management.

An IT investment portfolio is a collection of an organization's IT investments. Individual business units within an organization have IT investment portfolios as well, which are a subset of the corporate level portfolio.

IT Investment Portfolio Management is the process of choosing the most appropriate mix of investments to ensure the maximum benefit to the organization, and prudently managing the mix by monitoring and assessing its performance. The DON IT Investment Portfolio Management Process includes:

- **Establishing a Pool of Investments:** Collecting basic information about portfolio candidate investments and documenting all applicable data elements in a database.
- **Building the Portfolio:** Carefully scrutinizing and validating a pool of proposed IT investments that are in various stages of their life cycles and providing consistent information to senior decision-makers so they can determine which investments provide the best mix to accomplish the mission of the organization.

- Assessing the Portfolio: Monitoring the performance of the portfolio to ensure the mission is being supported by the approved investments, investigating issues which impact portfolio performance, and making adjustments to problematic investments in the portfolio as necessary to ensure mission accomplishment.

Historically, IT investments have been managed independently, not as a compilation that supports an organization's mission. IT Investment Portfolio Management is intended to focus on the overall collection of investments and not on individual projects/programs. However, to successfully manage the portfolio, each IT project/program must be prudently managed. The management of individual IT projects was discussed in the previous section as part of the Capital Planning process. This guidance is not changed by the IT Investment Portfolio Management Process. The addition of a portfolio concept is to determine how well a program or project supports the organization's mission when part of a portfolio. This is accomplished through the use of standard portfolio criteria in the selection, management, and evaluation of projects/programs. The following analogy is provided to explain the differences between project/program management and portfolio management.

The Portfolio Management Train Analogy

An IT Investment Portfolio is like an old-fashioned train with an engine, passenger cars, dining cars, sleeper cars, mail cars, boxcars, refrigerated cars, flat bed cars, and other connected units. Each train has a mission to get from point A to point Z and to meet a schedule and the needs of the passengers and cargo.

Each unit or car has its own goal or mission. For instance, the mission of the refrigerated car is to keep cargo cold. The mission of the dining car is to make food available for passenger consumption.

The process of IT Investment Portfolio Management can be likened to the assembling and operation of a train:

The Train Yard (The Pool of Investments). Individual cars sit in a train yard before they are assembled in a train. All the cars in the yard are constructed with standard criteria so they can ride on the tracks, fit through the train tunnels, and connect with all the other cars.

Similarly, IT projects/programs must comply with standard architecture requirements and business requirements of the Clinger-Cohen Act (CCA), the DoD, and Secretary of the Navy Instruction 5000 series for major and non-major defense acquisition programs, and organizational requirements for non-major projects/programs in order to be considered for the portfolio.

Assembling the Train (Building the Portfolio). A railroad official determines which cars make up the train based on the mission of that particular train. For instance he uses refrigerated cars on a train when part of the mission is to haul cargo that needs to be kept cold. He approves a dining car as a part of his train when he knows the train will have passengers during meal times. He determines the size of engine needed for the train based on total number of cars, weight to be hauled, and terrain.

In the world of IT, a Senior Executive Committee decides which candidate projects/programs will provide the best mix to accomplish the mission of the organization. The IT Portfolio Management process provides these decision-makers the information they need to make wise decisions about their IT investments. This information helps them avoid duplication and achieve the best return on their investments.

Operating the Train (Assessing the Portfolio). In operating a train, the engineer communicates regularly with the conductor and the rest of the train crew to make sure the train is running safely, effectively, and efficiently toward its destination. If a particular car develops a problem with one of its wheels, the engineer detects drag on the train and investigates the source of the problem. If the problem wheel cannot be fixed en route, the engineer removes the problem car from the train at the next station.

An IT portfolio must go through a similar monitoring process. If an issue arises in the performance of the portfolio, the engineer of the portfolio, the Investment Working Group, investigates, identifies the project/program causing the problem, and determines possible solutions or alternatives. The Investment Working Group presents these to the Senior Executive Committee who decides whether to continue the project/program as is, to fix the problem retaining the project/program in the portfolio, or to remove the project/program from the portfolio. During this monitoring phase, the Investment Working Group communicates with the project/program managers just as the engineer communicates with the conductor and crew.

Portfolio Versus Project/Program

Existing business processes for IT focus on projects and programs. These processes help ensure the IT projects/programs are on target with respect to mission, cost, and risk. Using the train analogy, railroad personnel evaluate whether a car operates correctly and does what it was designed to do.



IT Investment Portfolio Management gives senior decision-makers an opportunity to view the bigger picture. The focus is on the entire portfolio as opposed to the individual projects/programs. Decision-makers have the information they need to ensure that they have the best mix of IT projects/programs to accomplish their organization's mission.

A mature investment process requires discipline, executive management involvement and accountability, and focuses on risks and returns using quantifiable measures. Senior managers with programmatic responsibility in key business areas should be involved directly in prioritizing and selecting the IT projects/programs their organization will pursue. Decisions made related to IT investments must be made on quantifiable data and sound judgments related to the importance of one project/program over another.

The IT Investment Portfolio Management Guide is focused on IT investments related to various organizational levels. It demonstrates a process that a typical DON organization goes through in order to manage a portfolio of IT projects/programs. The organization's portfolio will consist of those projects/programs with a meaningful relationship to the

organization's mission. The expected outcome of implementing the process is a portfolio containing the best mix of prioritized IT investments based on criteria established by the organization's top level management. Organizations have the responsibility and authority to tailor the process to best support their needs and still comply with applicable legislation.

IT INVESTMENT EVALUATION HANDBOOK



The Evaluation phase is the third step in the continuous Capital Planning process. It closes the loop between the Selection and Management phases (see Section 8.1) by assessing actual system and management performance. While this phase is primarily thought of in terms of Post Deployment Reviews (PDRs) of newly deployed systems, in reality it also includes the periodic evaluations of ongoing operational systems.

The need to evaluate a system's ability to effectively meet the organization's mission needs, both functionally and economically, does not end at deployment. Rather, it is a *continuous process* to ensure that the system still supports both the end users and the mission needs of the organization.



An effective evaluation process not only assesses the success or failure of a newly deployed system or the continued effectiveness of existing operational systems, but also serves as a powerful knowledge tool. It provides insight into the strengths and weaknesses of the processes and procedures performed in the Selection and Management phases of Capital Planning. The ability to ensure future investment success is directly related to identifying strengths and weaknesses in our management processes via lessons learned and taking corrective actions to make improvements.

The IT Investment Evaluation Handbook was developed for the sole purpose of providing a recommended approach for conducting evaluation reviews. It applies to Automated Information Systems (AIS) and National Security Systems (NSS) Information Technology (IT) investments. It does not apply to IT that is embedded in weapons systems. The processes and procedures included in the handbook are intended to serve as guidelines. Organizations can add, modify, or tailor steps based on dollar amount, complexity, and local command requirements.

GUIDE FOR DEVELOPING AND USING IT PERFORMANCE MEASUREMENTS



One of the underlying tenets in the Department of the Navy is the ability to focus resources on IT investments that support the warfighting mission by providing secure information when and where it is needed. It is also manifested by focusing on IT investments that improve the mission and strategic objectives of all DON organizations, afloat and ashore, that directly or indirectly support the warfighting mission. The Government Performance and Results Act of 1993 (GPRA) directs that agencies report performance through measures that relate to their strategic goals. The CCA of 1996 further directs that agencies manage IT using performance measures that indicate how the IT supports organizational missions.

The process for developing and managing IT performance measures is an iterative one that begins with the definition of the investment and involves constant refinement and management throughout the life cycle of the asset. Figure 8.2-1 illustrates the process.

Step 1 - Define IT Investment. Review the Mission Need Statement, Operational

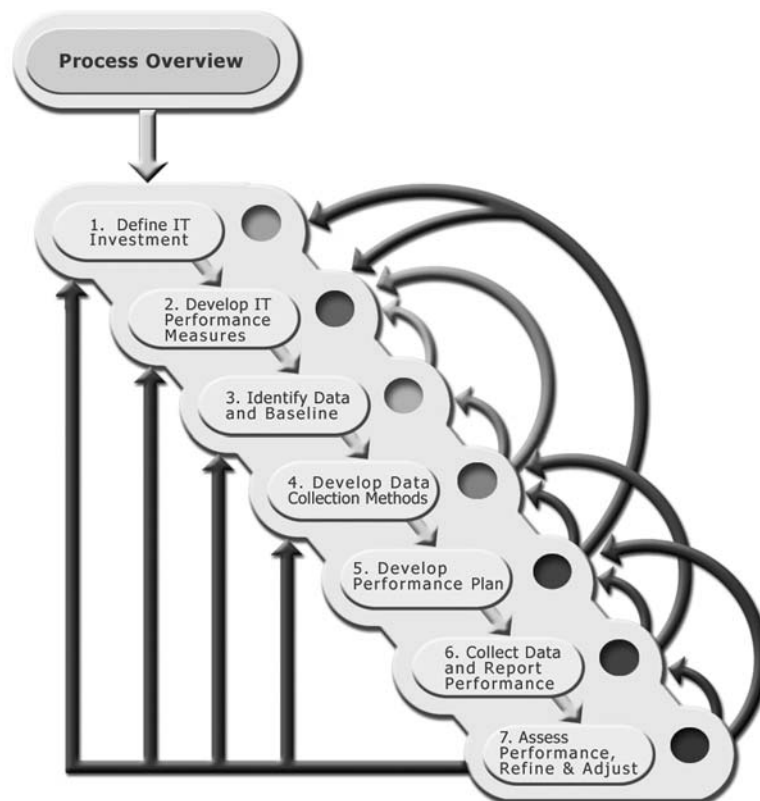


Figure 8.2-1—The process for developing and managing IT performance measures is iterative, beginning with the definition of investment and requiring constant refinement throughout the life cycle of the IT asset.

Step 2 - Develop IT Performance Measures. Develop objectives, associated measures, and actions to achieve the objectives, within each of the five Balanced Scorecard perspectives.

Step 3 - Identify Baseline Data. Identify data that already exists and the requirements for the collection of new data that will be used to support the baseline of information required by the measures developed in Step 2.

Step 4 - Develop Data Collection Methods. Develop methods and procedures for collecting, storing, and updating the data identified in Step 3 to satisfy required reporting frequencies.

Step 5 - Develop a Performance Plan. Develop a plan that describes how the organization will review objectives and measures developed for the IT asset, and how corrective actions will be taken to achieve intended targets. Corrective actions can involve such things as modifying internal processes to more effectively use the investment or taking action to continue, modify, or cancel based on the investment's ability to meet its intended objectives.

Step 6 - Collect Data and Report Performance. Begin collecting and updating the data as determined in Step 4. The data should be displayed in a manner, and with the required frequency, to effectively evaluate actual performance of the investment in comparison to the target performance for each measure.

Step 7 - Assess Performance, Refine, and Adjust. Take the corrective actions identified in the Performance Plan from Step 5 based on periodic reviews of the reports from Step 6.

The Balanced Scorecard, using the process described in the *DON Guide for Developing and Using IT Performance Measures*, substantially increases the likelihood that:

- Investments will be linked to overall mission support and improvement.
- Realistic objectives will be considered for IT investments.
- Actual performance of the investment will meet or exceed its intended purpose.
- Corrective actions will be taken in a timely fashion if performance requirements are not met.

It provides a model for ensuring that the investment will be continually evaluated from the perspective of the customer and the stakeholder and will also be continually evaluated from the financial perspective. The model helps ensure that objectives and measures are evaluated relative to the perspectives of learning and growth and internal processes within the organization. From this standpoint, it is a far better method of measuring performance as compared to traditional cost and performance measures. The real value to the DON is the model's strength in increasing the probability that IT investments will lead to improved mission performance and information superiority.

8.3 Enterprise Licensing

Teamwork, collaboration, and selfless hard work across multiple organizations and functions is essential to achieving the full benefits that Enterprise Licensing of software can bring. These include cost avoidance, savings and ultimately, the ability for the Enterprise to manage software as an asset. We have only scratched the surface.

—Floyd Groce, Enterprise Licensing Team Leader

BACKGROUND

Enterprise Licensing is an essential tool for the Chief Information Officer (CIO) to use in achieving successful Enterprise integration. As a tool, Enterprise Licensing is used to coordinate multiple information technology (IT) investments and leverage the buying power of the Enterprise for commercial software products. By consolidating software requirements and negotiating Enterprise Agreements with software vendors, the Enterprise realizes significant Total Cost of Ownership (TCO) savings in software acquisition and maintenance. The goal is to develop and implement a process to identify, acquire, distribute, and manage software entitlements at the Enterprise level.

The focus of Enterprise Licensing is on the fundamental problem with procuring software for the Enterprise: the high price and expense of software acquisition, distribution, training, maintenance, and support. Organizing the effort is critical to success, and a team approach is used to include a cross-section of activities and functions. In addition, lead departments are assigned for each Enterprise software area to permit a focused approach and allow specialization in a software product area. The team approach is a proven method to operate across organizational lines, leverage team expertise, and include the private sector in developing innovative solutions to multifaceted acquisition problems. In addition, Enterprise Licensing incorporates eight principles in a Concept of Operations to reduce risk and improve chances for success:

- Provide coordination and interface.
- Support collaboration across organizational departments.
- Provide expert contracting and acquisition advisory resources.
- Support rapid technology change.
- Improve information support to the Enterprise.
- All volunteer participation.
- Achieve economies and efficiencies in IT investments across the Enterprise.
- Facilitate accelerated implementation of critical systems and capabilities.

Savings of up to 70 percent were achieved on Section 508 Web site correction tools using the Enterprise Licensing approach.

IMPLEMENTATION AND OPERATION

At the core of Enterprise Licensing is the concept of an Enterprise Agreement combined with a streamlined contracting process. One approach that has been successful for establishing an Enterprise Agreement is a Blanket Purchase Agreement (BPA) placed against a General Services Administration (GSA) schedule with a software manufacturer or reseller authorized by the software manufacturer to resell the software to customers. This recognized best practice leverages the favorable GSA contract terms and conditions with quantity price discounts negotiated by the Enterprise Licensing Team.



The Team targets common-use commercial software products and software publishers. Before engaging one or more software resellers in discussions, a best practice is to work first with the software publisher(s) to understand their pricing and licensing model, including terms, conditions, and product use rights. The Team may need to meet with the software publisher several times to reach an understanding of the model as well as each party's incentives for entering into an Enterprise Agreement and maintaining it over time. If needed to help establish the business case, the Team enlists the help of the software publisher in identifying the installed base of their software in the Enterprise. This helps validate demand and can provide additional negotiating leverage so that the installed base of software can be "grandfathered" into the Enterprise Agreement. Following this approach, the Enterprise Licensing Team can achieve savings for current customers as well as discounts for future software investments. As a result of this process, Enterprise Licensing has produced some significant success stories, measured by ease of use for both large and small customers, efficiencies in procurement, tracking of software purchases, and substantially reduced prices.

Significant savings were achieved by purchasing a "virtual inventory" of Microsoft server products.

The benefits of Enterprise Licensing have also been shown in acquiring IT hardware and services in addition to software products. For example, significant savings have been achieved with expanded access to the premier IT research and advisory service companies through the use of Enterprise Agreements. These research and advisory services facilitate adoption of industry best practices and have resulted in millions of dollars of savings and cost avoidance.

One note of caution for organizations proceeding down an Enterprise software initiative-like path. Taking a step back from the view inside the Department of the Navy (DON) or Department of Defense (DoD) and looking at Enterprise Licensing efforts from the vendor's stand point, there are often conflicting agendas. The DON is trying to maximize the value of the awards made on behalf of the government, simultaneously minimizing the cost of these efforts on taxpayers. In short, the DON is trying to show good fiscal management.

The vendors, on the other hand, are primarily focused on profit and loss. The vendors have both an internal sales force and channel sales partners, and each of these has a quarterly sales quota and yearly incentive plan that typically does not match what the government wants to do. Often times, the negotiation period can be difficult. The software company is concerned both from a revenue and sales force (internal or channel) perspective. Will entering this agreement put the sales force on the street? Will it affect the overall relationship with the channel partners? Is the forecasted revenue quota from the boss still achievable? These are real-life concerns. This is where the art of negotiation comes into play. If both the government and the vendor can walk away from the negotiating table feeling satisfied, it's a win-win situation.

INNOVATION AND ADAPTABILITY



Enterprise Agreements can be used to better integrate government and commercial business processes. Under Enterprise Licensing, all Enterprise Agreements are open for use by contractors supporting the government. In this way, the government shares in the savings realized by our contractors in the purchase of software for government contracts. In addition, Enterprise Agreements should include requirements to ensure products are compliant with the Enterprise's IT standards, thereby promoting interoperability. Other commercial best practices should be identified and adopted, including assigning responsibility for negotiating Enterprise Agreements only to offices with demonstrated specialized knowledge and expertise.

The Enterprise License process and end products are designed for flexibility, and are suited to multiple operating environments that support the mission of the Enterprise. The Enterprise Agreement model, itself, is carefully constructed to better allocate and manage risk between the parties. As a risk management tool, the Enterprise Agreement protects the Enterprise's interest while reducing TCO and improving performance and schedule. The end result is a shorter acquisition lead-time to meet the customer's needs faster, better, and cheaper.

Special solutions discounts for Oracle products have been achieved up to 84 percent off GSA Federal Supply Systems prices.

Enterprise Licensing can also improve the software acquisition system with a focus on better use of buying professionals. Front-line procurement and industry personnel should be consulted to identify best contracting methods to use. In addition, selected customer groups should be surveyed to ensure that the methodology is responsive to their needs.

The Enterprise should also devise a marketing program to advertise Enterprise Agreements to their customer groups. This program includes appropriate marketing brochures, publications, and presentations at technology symposia. Additionally a system should be developed to ensure the results and lessons learned from each Enterprise Agreement negotiation are captured in a database for future reference.



Enterprise Licensing success depends on establishing an Enterprise process that remains viable to support the organization mission and satisfies the needs of its customers. One of the tools we have used successfully is the Department of Defense Financial Management Regulations, which allows the use of the Defense Working Capital Funds to finance the purchase of software licenses “up front” under the Enterprise Software Initiative. The DON Enterprise Licensing Team has used this authority to purchase a “virtual” inventory of Microsoft server and Oracle database products and then made these products available for ordering online through various virtual IT stores accessible to the customers. This method resulted in a savings of several million dollars for DoD customers. This has allowed DON to use leading edge Internet and electronic commerce technologies to implement improved business processes. Web technology is incorporated in the Enterprise Licensing business processes to facilitate improved coordination and information exchange among Team members. Finally, regular reviews of the status of Enterprise Agreements are conducted for potential improvement, technology and product refreshment, additional consolidation, and expansion of customer base.

PEER RECOGNITION

From the government’s perspective, Enterprise Licensing efforts have received a great deal of notoriety. In 1999, the DoD Enterprise Software Initiative won the 1999 Information Resources Management Conference Award as the Best Federal IT Team. In 2000, it was a Finalist for the 2000 Excellence in Government Award. Separately, the DON Enterprise Licensing Team was nominated for the 1999 David Packard Excellence in Acquisition Award, received the 1999 Defense Acquisition Executive Certificate of Achievement, and the Department of the Navy Fiscal Year 2000 Competition and Procurement Excellence Award. For the employees that work on both the DoD and DON Teams, this recognition brought a huge sense of personal satisfaction that the efforts they undertook did not go unnoticed by their peers across government.

SOFTWARE ASSET MANAGEMENT (SAM)

When an Enterprise implements an Enterprise Licensing program, the Enterprise must also understand the need for Software Asset Management (SAM). SAM is a process within IT asset management that brings together the physical, financial, and contractual attributes of software to enable the delivery of cost-efficient, timely business solutions. In essence, it is the process of proactively managing software as an asset of the organization. It is a practical business approach that supports other essential processes such as IT capital planning, and property, plant, and equipment accounting. Like Enterprise Licensing, it is also a complex undertaking that demands leadership from the highest levels of the Enterprise and participation from virtually all executives, managers, and professional employees.

Sybase’s limited “Golden Disk” for Adaptive Server Enterprise (ASE) entitles DoD to unlimited seats at 64 percent off GSA Federal Supply Systems prices.

SAM embodies IT Capital Planning Process methodology, but extends the methodology to make Enterprise software use a management consideration. The traditional approach to software management in many Enterprises is deficient in two primary areas. First, software tends to be viewed and managed as an expense or consumable instead of an organizational asset. Secondly, traditional management focus is from a program or functional perspective, and not an Enterprise or organizational perspective. This approach causes overbuying of licenses (entitlements), and prevents effective use of software through resource sharing and reuse. Liability for software misuse, i.e. piracy, is also a major consideration for an organization to manage its software resources as Enterprise assets.

SAM should be implemented through a framework of recommended procedures, methodology, and techniques that are used to establish an Enterprise-wide process. This framework is intended to provide guidance for the line manager and other personnel directly responsible for evaluating, selecting, and managing the organization's software assets. It should set forth a practical, flexible, and adaptable approach to support unique organization mission requirements. The implementers of SAM must exercise judgment in making appropriate variations and adaptations as necessary to the framework procedures to fit the needs of the Enterprise.

CONCLUDING THOUGHTS

The Enterprise Licensing process has proven to be an essential tool in Enterprise integration, and has had a significant, positive impact across the DoD. By leveraging buying power, the DoD realizes significant savings in TCO, ensures IT investments comply with Enterprise-wide standards, architectures, policies, and procedures, and enables ordering and tracking of licenses through a common, Enterprise-wide coordinated process.

8.4 Metrics

Metrics focus leadership attention. The Balanced Scorecard approach allows senior leaders to assess the health of the organization through outcome-based performance measures.

—Don Reiter, Communications and Outreach Team Leader

BACKGROUND

Performance measurement is a key component of effective management. A continuing theme in management theory and practice is, that which gets measured is which gets attention.

Performance management is the use of performance measurement information to effect positive changes in organization culture, systems, and processes. It provides a framework to:

- Help managers establish agreed-upon performance goals.
- Allocate and prioritize resources.
- Inform managers about the needs to change current policy or program directions to meet those goals.
- Share results of performance in pursuing those goals.

Performance measurement is the process of assessing progress toward achieving predetermined goals, including information on the efficiency with which resources are transformed into goods and services (outputs), the quality of those outputs (how well they are delivered to customers and the extent to which customers are satisfied), outcomes (the results of a program activity compared to its intended purpose), and the effectiveness of operations in terms of their specific contributions to mission objectives.

Performance measures are the standards used to measure success in achieving an objective. They describe the precise measurement that will generate a quantitative (or qualitative) indicator that explicitly or implicitly indicates progress towards achieving the objective.

Successful managers use performance measures to:

- Improve mission performance.
- Support budget and Program Objective Memorandum (POM) submissions and justifications.
- Substantiate requirements for IT.
- Report on the success and measure the value of IT investments.
- Develop benchmarks for future comparisons and for others to use.

The Government Performance and Results Act of 1993 (GPRA) directs that agencies report performance through measures that relate to their strategic goals. The Department of Navy (DON) Information Management/Information Technology (IM/IT) Strategic Plan delineates the Department's strategic IM/IT goals. The Clinger-Cohen Act of 1996 (CCA) further directs that agencies manage IT using performance measures that measure

how well the IT supports their missions. In response to this direction, the DON Chief Information Officer (CIO) developed two guides for measuring IT performance. These metrics guides cover IT (*The Guide for Developing and Using IT Performance Measurements*) and knowledge management (*Metrics Guide for Knowledge Management Initiatives*).

Performance measures are used to support the selection, funding, acquisition, deployment, maintenance, and enhancement of an investment. Focusing on dollars, performance measures are developed during all phases of IT Capital Planning (see Sections 8.1 and 8.2). In this section, performance measures are discussed for IT in general and for knowledge management initiatives specifically.

IT PERFORMANCE MEASUREMENTS

One of the underlying tenets in pursuit of information superiority in the DON is the ability to focus resources on IT investments that are the most effective in achieving that superiority. This is manifested directly by investing in IT that supports the warfighting mission by providing secure information when and where it is needed. It is also manifested by focusing on IT investments that improve the mission and strategic objectives of all DON organizations, afloat and ashore, that directly or indirectly support the warfighting mission.



In an IT context, performance measures provide the information needed to assess how well IT investments support the organization's missions, goals, and quantitative objectives. Performance measures focus on achievement. Since the concern is on satisfying mission objectives, a few, well chosen measures that emphasize the vital and critical success factors of the mission are better than a large number of system-oriented output measures. Performance measures provide the means to assess effectiveness and efficiency. Effectiveness is doing the RIGHT things; efficiency is doing things by employing the BEST use of available resources.

Many managers understand that the context or level of their IT investment will drive the information requirements for their performance measures. They also know that they need to focus on the factors they can influence or control. Recognizing that different management tiers need different types of information to make business decisions, there are three tiers or levels of performance measures defined by the DON IT Capital Planning Guide to satisfy these needs: enterprise investments, functional investments, and infrastructure investments.

The DON CIO has developed the IT Capital Planning and Portfolio Management processes to assist DON organizations with their responsibilities related to selecting, managing, and evaluating IT investments to be compliant with GPRA and CCA. The *DON Guide for Developing and Using IT Performance Measurements* supplements the IT Capital Planning and Portfolio Management processes by providing an outcome-oriented method for measuring the impact of IT investments on the organization's mission, goals, and objectives. To achieve this end, the guide recommends the use of Kaplan and Norton's Balanced Scorecard, modified for the Federal Government. Figure 8.4-1 summarizes the who, why, what, when, and how of the performance measurement process.

The linkage of IT investments to desired agency outcomes is a step beyond traditional measures that have focused on IT system output, e.g., cost, performance, schedule, speed of operation or response times. By law, executive agencies must implement IT performance measurement, consider outcomes in acquisition decision-making, and conduct performance measurement to determine how well goals are met.

Performance measurement enhances current DON Enterprise IT processes by helping senior managers focus on true mission impacts for proposed and existing IT investments. Funding is directed to those systems best meeting the DON strategic goals and objectives, and which produce the best performance for the money spent.

When are IT Performance Measures Developed?

Performance measures are used to support the selection, funding, acquisition, deployment, maintenance, and enhancement of an investment. Performance measures are developed during all phases of IT Capital Planning.

During the selection phase of the IT Capital Planning process, the DON adopted performance measures as one of the minimum criteria to be considered in making IT investment funding decisions. These criteria include:

- Savings, cost avoidances, or performance improvements.
- Relevance to mission or business area goals.
- Risk, expressed as minimal Return on Investment (ROI), project longevity, or technical risk.

The requirement to base IT investment funding decisions on the specified minimum decision criteria applies not only to budgeted IT investments but also to those investments which surface during execution. Decisions to fund these emergent IT investments during execution must be supported by documentation addressing the minimum criteria as the basis for funding approval.

Performance measures are used during the management phase of the IT Capital Planning process, for measuring ongoing IT projects against their projected costs, schedules, and benefits and for taking action to continue, modify, or cancel them. Reviews should be performed at regular intervals during the life cycle of an IT investment to ensure that it continues to meet its mission objectives cost-effectively. The decision to continue, modify, or cancel an IT investment project should be a deliberate management decision, documented and justified by a review and analysis of the measures.

During the evaluation phase of the IT Capital Planning process, managers evaluate performance, comparing actual to planned achievement, identifying the reasons for variance, and identifying appropriate corrective actions. The evaluation phase of Capital Planning assesses the technical and functional performance of an investment, its cost effectiveness and contribution to mission, and how well the investment was managed to delivery. IT investments should be subject to regular scrutiny through the application of performance measurements, which provide the feedback necessary to assess the continued effectiveness of the process, as outlined in the *DON IT Investment Evaluation Handbook*.

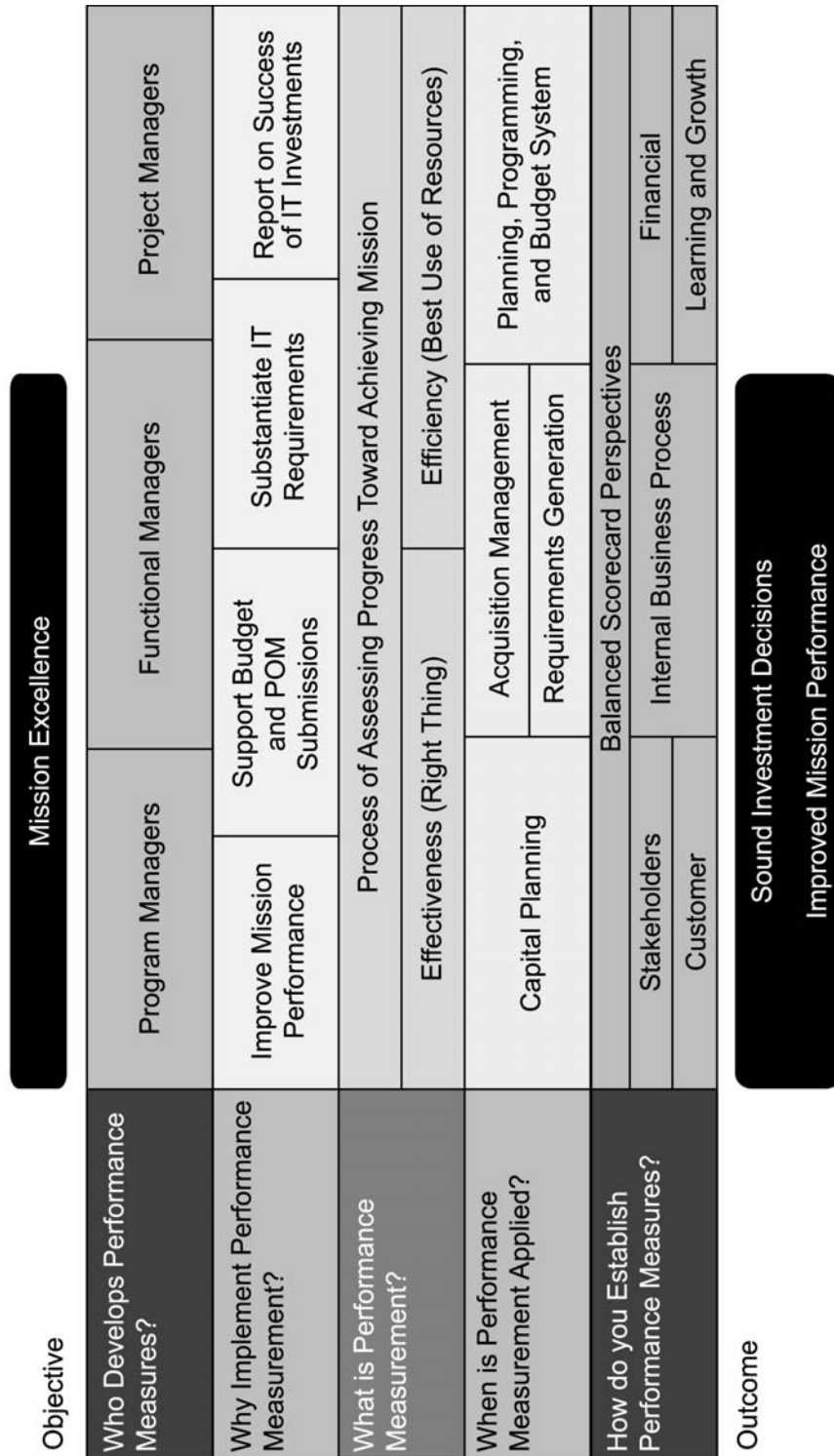


Figure 8.4-1—The Who, Why, What, When, and How of the IT Performance Measurement Process.

During the selection phase of the IT Capital Planning Process, when the actual investment funding allocation decisions are made, managers assess whether the IT performance measures indicate that the investment is meeting its mission objectives. In the DON, this occurs during the programming or POM development phase of PPBS when resource sponsors make decisions related to policy implementation, and program levels, program direction, and affordability are addressed based on guidance flowing from the planning phase. As each project is reviewed at various stages during its life cycle, decisions are made regarding the future of the project. Decisions may be made which call for the suspension of funding or make future funding releases conditional on corrective actions being taken. The Planning, Programming and Budgeting System (PPBS) process is associated with the selection phase of IT Capital Planning.

During the Acquisition process, performance measures are developed and monitored routinely by the program manager and presented during milestone reviews to Milestone Decision Authorities (MDAs). If necessary, the measures are adjusted periodically to reflect realistic targets based on experience. During milestone reviews, measures are used as one of the critical factors in deciding whether to continue, modify, or terminate a particular program. The Acquisition process is associated with the management phase of IT Capital Planning.

The DON *Guide for Developing and Using IT Performance Measurements*, discussed in Section 8.2, walks the user through the process of developing performance measures.

KNOWLEDGE MANAGEMENT METRICS



Knowledge Management (KM) provides a methodology for creating and modifying processes to promote knowledge creation and sharing. These processes are not new independent KM business processes but processes developed by applying the KM methodology to core organizational applications. KM, implemented by and at the organizational level, and supporting empowerment and responsibility at the individual level, focuses on understanding the knowledge needs of an organization and the sharing and creation of knowledge by becoming part of the fabric of the organization.

Connecting people is the primary focus of KM initiatives. Indeed, it is essential to understand that KM is not about simply increasing access to information. On the contrary, access to large amounts of information is good when there is ample time to peruse it, but this access does not provide quick answers. KM seeks to provide these answers through a balance between stored, succinct, and directly pertinent information and links to other people who are likely to know how to help.

KM provides two major benefits to an organization. It improves the organization's performance through increased effectiveness, productivity, quality, and innovation and it increases the financial value of the organization by treating people's knowledge as an asset similar to traditional assets like inventory and capital facilities. Each of these benefits has distinct qualities that can be measured, such as the effectiveness of sharing and the intrinsic value of knowledge assets. However, since DON organizations execute and support Fleet operations, they are primarily interested in the operational mission performance

improvement benefit of KM. Consequently, the DON CIO developed a guide that focuses on determining effective performance measures to assess the organization's current status in becoming a Knowledge Centric Organization (KCO). At every stage in the journey, metrics provide a valuable means for focusing attention on desired behaviors and results.

THE ROLE OF METRICS IN KM

Performance measures for KM have several objectives:

- To help make a business case for implementation.
- To help guide and tune the implementation process by providing feedback.
- To provide a target or goal.
- To measure, retrospectively, the value of the initial investment decision and the lessons learned.
- To develop benchmarks for future comparisons and for others to use.
- To aid learning from the effort and developing lessons learned.

Performance measures should be designed and implemented to reflect organizational goals and objectives. KM is a strategic business process that enables other critical business processes. Therefore, it is important to focus measures (and the entire initiative) on factors that affect the ability to achieve strategic objectives. The Government Performance and Results Act (GPRA), passed in 1993 and enacted in 1997, brought to the forefront the concept of applying performance metrics to link funds availability and program effectiveness in Federal agencies. This legislation requires agencies to develop strategic plans and performance metrics to tie their success in achieving strategic objectives to their Congressional funding. The performance plan must specifically define performance measures, required resources and processes, and how the measures will be used. These measures must directly relate to the performance goals, which are classified as outcome changes in the goal targets, and output changes in the specific activities undertaken to achieve the goal.

Similarly, the KCO model uses three types of metrics to assess different levels of KM impact—namely outcome (Enterprise or overall value), output (project or task), and system (technology tool). However, care must be used to “pick the right measure” just like “picking the right tool,” as outlined in the National Performance Review report on performance measures. Based on a review of many high-performing organizations, this report identified several key factors in designing and using performance measures that are just as important to building a KCO. These factors include: using a few focused measures aligned to strategic objectives; measuring critical characteristics of the business processes; and recognizing measures as being only valuable tools and not the products of the project.

The perspectives of the customer, department, organization, and individual in an Enterprise are critical to its success and need to be incorporated into that success. The implication of this for KM metrics is critical—when thinking about metrics, it is important to identify who is likely to use the performance measurement information. Potential users include strategic decision-makers, special project decision-makers, funding and approval stakeholders, government agencies involved in approval or regulation, or customers.

Measures should be in terms that are familiar to the stakeholder. For this reason, you may find that there are several different metrics that need to be captured for your initiative. There is no one “right” set of measures for KM initiatives and most KM initiatives will require a combination of measurement types and classes to effectively communicate with the key stakeholders. The measures must reflect the overall mission and strategy of the organization.

The DON CIO developed a *Metrics Guide for Knowledge Management Initiatives* that describes several types of metrics that have been effectively used in KM and other business projects. These applications differ in how people perceive knowledge and the timeliness with which they need to access and act upon the knowledge. Three primary classes of business objectives are used to characterize KM initiatives and to help design the proper mix of performance measures: Program and Project Management; Program Execution and Operations; and Personnel and Training.

Performance measures support decision-making and communication throughout an organization to understand the progress, efficiency, value, and strategic alignment of KM projects. Measuring and documenting the results of KM initiatives provides a powerful way to link the application of KM to bottom-line business outcomes. Developing a return on investment for KM presents unique challenges in that the return may take several years to materialize, and often the results tend to be more qualitative than quantitative. In general decision-makers and those charged with business investments expect to be presented with the anticipated return on investment prior to signing off on a project. When it comes to demonstrating results, most of us are more comfortable with quantitative measures—hard numbers which make it difficult to refute the investment value.

One of the most important things to keep in mind about KM initiatives is that performance measures are just a starting point; it takes a far more serious, strategic commitment to make organizations truly effective. To achieve the objectives of a KCO, the KM initiative must be continuously assessed at all levels of the organization to ensure that the required actions and changes are being made and redefined, if necessary. This is a continuous process.

THE KM MEASUREMENT PROCESS

The measurement process is composed of several steps to clearly identify what should be measured, how to measure it, and how to use the measures. This process is shown in Figure 8.4-2 as a series of questions that helps guide you through the decisions of defining, choosing, and using the metrics.

The KM measurement process includes thinking about and answering the following questions:

Who are the Stakeholders and What do They Need to Know? An important step in the measurement process is to identify who will use the measures. This can be a KM project champion, officers and managers, participants, funding and approval officials, internal customers, supply industries, and other stakeholders. A useful technique is to brainstorm a

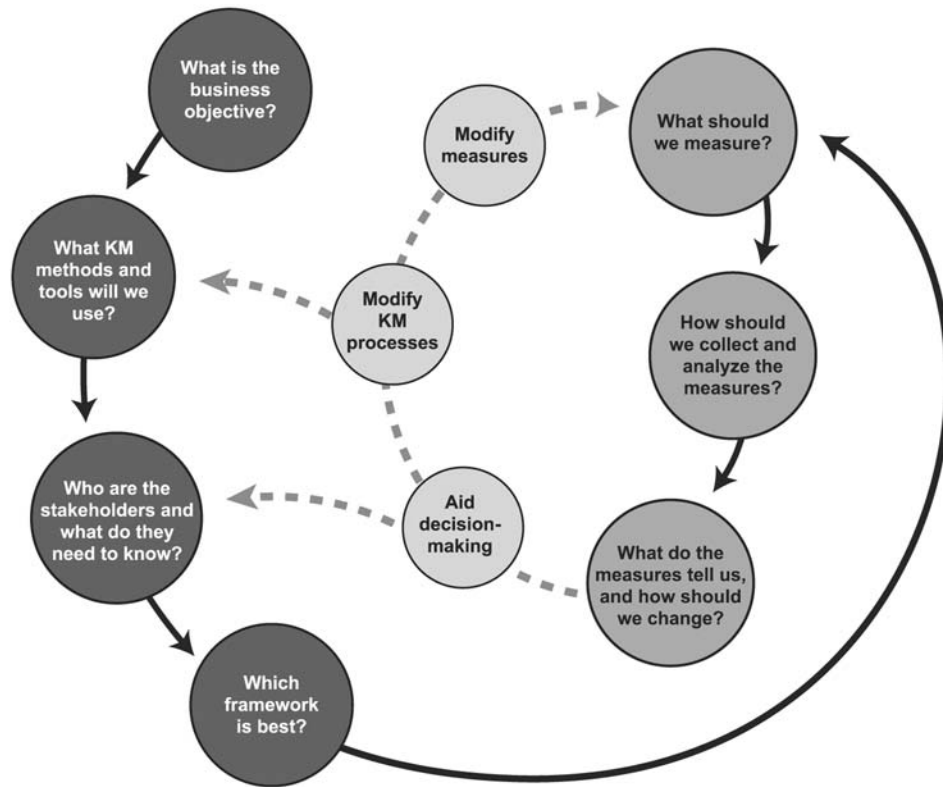


Figure 8.4-2—The KM performance measurement process is supported by a series of questions that helps guide you through the decisions of defining, choosing, and using the metrics.

list of all possible audiences for the measures and then review the list to remove duplicates and add any positions or organizations not included previously.

However, be careful not to include such a large number or wide range of people that it will be too difficult to accommodate all of their concerns and needs. A key part of defining the business objective and KM methods (steps done before the metrics process begins) is to focus the KM initiative on specific organizational needs. These activities should have identified the primary stakeholders, even if only in a general sense, and this list can help consolidate the final list into stakeholders who are substantially connected to the initiative.

Next, identify the stakeholders' most important questions and the decisions they will make in order to determine exactly what information they need to glean from the measures. They may want to determine how valuable the knowledge assets are to the organization in practice, how effective the KM system is in enabling knowledge sharing and reuse, or both. Thus, measures have to be tailored to each need.

Which framework is best? A framework helps ensure the metrics are aligned to the project objectives and the organization's strategic goals. A framework is a more useful way to convey the measures than merely listing them. A framework can show how actions

contribute to overall goals, the mechanisms by which actions produce benefits, the rationale for conducting the KM project, and, in some cases, provide an analytical tool for making investment trade-offs.

There are several ways to construct a framework using organization schemes such as a balanced set of measures, benchmarking, target setting, matrices, hierarchies, flow diagrams, and even management systems. The best choice depends on which ones make it easy for your team to gauge and understand the costs, benefits, relationships, and impacts of the KM processes and measures to each other and to organizational objectives. The key characteristics of some of these schemes relating to KM initiatives are:

- Flow—traces KM activities to impacts and related measures, and is good for showing how KM activities produce benefits.
- Matrix—good for showing the rationale for prioritizing and selecting among a group of KM projects, and is often used in portfolio management.
- Causal loop diagrams—show the cause and effect structure of a system through the relationships between its key parts. These diagrams can help you understand complicated relationships where many factors interact and there are few, if any, simple linear cause-effect relationships.
- Balanced Scorecard—aligns measures with strategies in order to track progress, reinforce accountability, and prioritize improvement opportunities.

What should be measured? The most important characteristic to consider when choosing or defining a KM performance measure is whether the metric tells if knowledge is being shared and used. Measurements for KM initiatives can be quantitative or qualitative and, in general, a measurement program should include both types of measures. Quantitative measures all use numbers and typically provide hard data to evaluate performance between points (such as last month to this month), or to spot trends. For example, you can collect quantitative data on Web site statistics, the number of hours spent on a particular task, or the percentage of equipment removed from operational status for repairs. Qualitative measures use the situation's context to provide a sense of value and are referred to as soft data. These measures include stories, anecdotes, and future scenarios. When it is difficult to capture meaningful quantitative measures, such as the value to the individual for being a member of a community of practice, a story from a member about how the community helped him solve a critical problem can have as much or more impact on stakeholders. Qualitative measures can augment quantitative measures with additional context and meaning.

How Should Measures Be Collected and Analyzed?

As the measures to be used for KM initiatives are identified, a process for collecting these measures must also be identified. It is important to structure information gathering and probe deep enough to understand how decisions are made and the information that measures can provide to help decisions.

For system measures, look for automated data collection systems, such as tools that measure Web site accesses and wait times. System performance logs also provide valuable system measures. For output and outcome measures, manual counts, estimates, or surveys may be used. Though surveys are considered a source of soft data because they measure perceptions and reactions, they can be quantitative.

Other techniques that can be useful are interviews or workshops, structured program flows, agency/organization documents, and meetings involving the performing organizations and stakeholders.

What Should We Do With these Measures?

The measures collected should help determine the effectiveness of the KM projects. In collecting measures, you should ask: Are people using knowledge? Are people sharing meaningful knowledge openly? Have people participated during the rollout while there was a great deal of fanfare and then stopped? Are there any anecdotes showing that people became more efficient or solved a problem faster because of the knowledge?

For all of these questions and other indicators, ask why it happened or had that response. Even without a firm answer, the search for an answer will most likely yield valuable insights and ideas on how to improve KM projects. Collect and prioritize these new ideas and go back to the original plans and assumptions to see if they need to be changed, as depicted in Figure 8.4-2. It is normal that several measures will need to be modified. This is a good time to assemble your team and build a consensus on what should be changed, how to change it, and when to introduce the changes. Also, the measures and framework should be updated to make sure they are tightly coupled to the new KM plans. Above all, remember to measure desired future results in addition to past performance.



Managing Change

Four years into the fully planned and implemented process of working toward building a world-class Chief Information Office (CIO), the Department of the Navy (DON) has been publicly recognized as a leader in the implementation of information technology (IT), information management (IM), and knowledge management (KM) in a complex United States Government organization. The Department's multifaceted change strategy will serve as a structured framework for exploring the initiatives, measures, and incentives that are making the mission of *putting information to work for our people* a reality.

The DON—comprised of both Civilian and Military personnel in the Navy Department, the Marine Corps, and the Secretariat—consists of approximately 800,000 Military personnel. At any point in time you might find 36 percent of the 315 ships in the total force on deployment and underway. That means approximately 46,000 Navy officers and Sailors and 34,000 Marines are away from their families and homes in defense of their country.

But the DON is larger still, with a diverse support organization scattered throughout government, industry, and academia around the world. This network of people and knowledge in support of National Defense has become more and more interconnected, and more and more complex, as the years have passed. And the decisions emerging from this interconnectedness are affecting the course of history.

So how do we change this complex organization that is the DON to meet the challenges of this new world of exploding information, increasing uncertainty, and growing complexity? Innovation is key. This chapter discusses the innovation life cycle and resistance to innovation, then takes a complex change strategy and distills it down to a dozen major change elements, sharing examples from the journey the U.S. Department of the Navy began four years ago.

OVERCOMING BARRIERS

Innovation is at the heart of sustained performance advantage. New ideas create the advantage, spread that advantage, and sustain that advantage. During this life cycle, information technology is the connective tissue that enables more effective and efficient innovation and promotes the opportunity for implementation at the Enterprise level (see Figure 9-1).

Every organization has some level of resistance to innovation. The ability to identify and overcome this resistance, coupled with an effective change management program, is paramount to the organization's success. Barriers to change come in many sizes and shapes. They include such things as allocations, scaling processes, organizational structures, size, organizational culture, and personal attitudes. Ultimately, the Institutional Will prevails, and how these barriers are addressed and overcome directly affect the reaction and acceptance of needed changes.

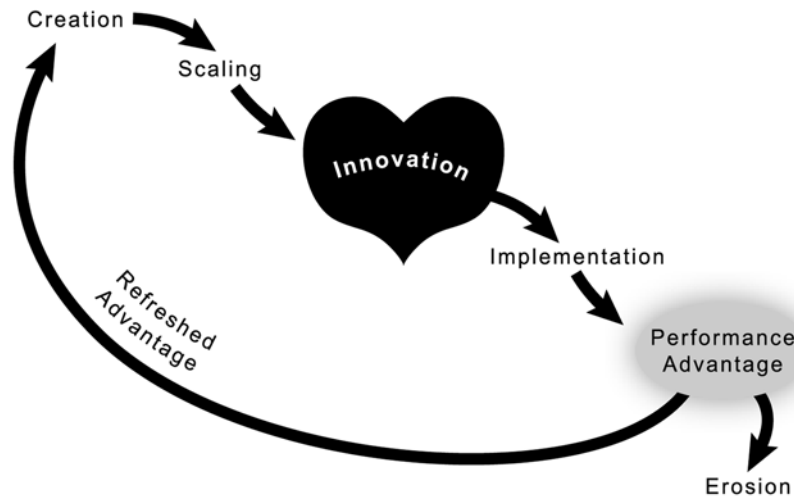


Figure 9-1—Information technology provides connective tissue for the Innovation Life Cycle.

Financial, acquisition, program management, career advancement, and incentive policies and structures in large organizations like the Department of the Navy may work against the easy implementation of innovative ideas. Mandates for security, return on investment analyses, and performance measurement are sometimes turned from their noble intent to serve as delaying tactics by organizations seeking to avoid implementing substantive change. In *The Wizard of Oz*, the Wizard tells Dorothy and her companions that before he could even begin to consider granting their wishes, they must undertake what he perceives as a hopeless task—bringing him the Wicked Witch’s broom. When these plucky over-achievers actually return with the broom, the Wizard is quick to begin back-pedaling on his end of the bargain. Similarly, new initiatives in the government are often subjected to onerous analyses, microscopically detailed return on investment calculations, and lengthy development timelines and approval processes that must be completed before a new idea can be implemented. Innovative managers are stymied in their efforts to effect real change while existing initiatives continue to be funded, even if results are less than desirable.

To a large extent, financial processes are geared to give a “bye” to the status quo, thus heavily biasing the organization to maintain the status quo rather than implement sweeping change. When the “status quo” gets a “bye,” an organization’s growth is stunted. Instead, the status quo must be constantly questioned and replaced if performance advantage is to be sustained.

Change innovation strategies fall somewhere on the continuum from continuous improvement to reengineering and beyond (see Figure 9-2). Continuous improvement denotes a large number of small innovations that reach from within to influence Enterprise change. Reengineering at the Enterprise level is accomplished through a small number of large innovations to rapidly facilitate change. An element of both strategies is necessary for optimum sustained change. To achieve this optimum positioning, the organization must manage internal and external barriers in the process of managing change.

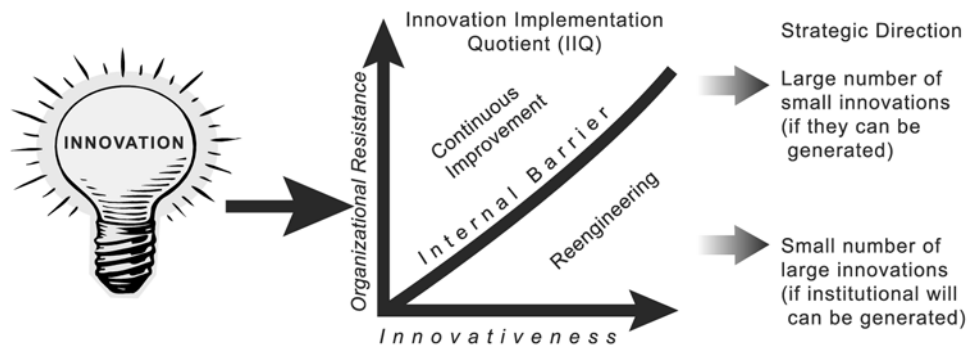


Figure 9-2—Innovation strategies for sustained advantage fall somewhere on the continuum from continuous improvement to reengineering and beyond.

THE DON CHANGE STRATEGY

The DON Change Strategy can be viewed in terms of orchestrating and implementing 12 specific elements. While change is a product of combining, integrating, and correlating these elements, each of these change elements will be addressed separately to facilitate understanding. These elements, detailed below, include: creating a shared vision; building the business case; demonstrating leadership commitment; facilitating a common understanding; setting limits; sharing new ideas, words and behaviors; identifying the strategic approach; developing the infrastructure; measuring and incentivizing; providing tools; promoting learning; and visioning an even greater future.

1. CREATE A SHARED VISION

In *The Fifth Discipline*, Peter Senge emphasizes the importance of a shared vision where employees participate in development of a corporate vision, and can then make decisions and take actions consistent with the directions set by senior leadership through the shared visioning process (Senge, 1990). In their research on consciousness, Edelman and Tononi identify the mechanism that provides unity to consciousness, thereby creating a continuous history of thought and a consistency of identity and action. This ability to maintain different parts of the brain in harmony and to pull them together in an organization is facilitated by constant and widespread communication (Edelman and Tononi, 2000).

The DON journey toward building a world-class CIO began with development of the DON IM/IT Strategic Plan. This plan was developed over a six-month period by hundreds of people who represented the different organizations and functional areas of the Department, and worked at every level of the Enterprise. The vision of the future presented in this first Strategic Plan was:

- An integrated, results-oriented Navy and Marine Corps team characterized by strategic leadership, ubiquitous communication, and invisible technology.
- An effective, flexible, and sustainable DON Enterprise-wide information and technology environment that enables our people to make and implement efficient and agile decisions.

- A Knowledge-Centric culture where trust and respect facilitate information sharing and organizational learning.

Nine strategic goals led the way for achieving this vision. The inclusion of success stories collected over the six-month development cycle solidified a common understanding of the goals and facilitated rapid implementation of the plan. See Chapter 2 for further discussion of the strategic planning process.

2. BUILD THE BUSINESS CASE

The starting point for the DON is the Naval mission. Information and knowledge have been critical to both the prevention and success of war since the beginning of man. Sun Tzu, the early authority on warfare strategy, said that what enables an intelligent government and a wise Military leadership to overcome others and achieve extraordinary accomplishments is knowledge. In the introduction to *Sun Tzu, The Art of War*, B. H. Liddell Hart states: “Sun Tzu believed that the moral strength and intellectual faculty of man were decisive in war, and that if these were properly applied, war could be waged with certain success” (Griffith, 1963).

Historically, technology has always been a determinate of success in warfare. The 1999 DON Posture Statement placed technology at the forefront of the Department-wide transformation to address tomorrow’s significant challenges. It positions the DON for sustained performance advantages through innovation. Specifically,

As we continue to navigate the uncharted waters of this new era, the Navy and Marine Corps need to harness technology and accept the resulting cultural changes to remain the world’s preeminent Naval force. Sustaining our ability to quickly implement new technologies and adapt to new requirements and missions will require an increasingly sophisticated array of forces and talented people. This is essential to our preeminence as a forward deployed, operationally proficient, and technologically advanced force, capable of responding anytime, anywhere from the sea.

When we use the word technology, the intent is how technology is used in support of the Naval mission. For IT, that means how information is managed and used.

A vision for Navy Knowledge Superiority emerged from a flag-level conference held at the Naval Academy in the fall of 1999. The realization of the value of KM to Naval warfighters at every level of the organization (see Section 5.2 “Knowledge Management”)—coupled with the historically given culture and respect for teamwork and unity—quickly validated the business case for KM. Today Knowledge Superiority is the second plank in the Defense maritime strategy, right beside the primary mission of forward presence that has been so important to Defense for the past 30 years.

3. DEMONSTRATE LEADERSHIP COMMITMENT

With the advent of Clinger-Cohen, each government agency was required to name a CIO. In the DON, the role of CIO was placed at the highest level of the Secretariat. This

strategic placement provided the visibility and funding necessary to champion IT, IM, and KM, and acknowledged the management of information and knowledge as integral to success of the Naval mission.

The integrated leadership team structure that participated in development of the IM/IT Strategic Plan—with representatives drawn from across the DON Enterprise—became the leadership team for implementation. A Board of Representatives was formed that included representatives from the Chief of Naval Operations, the Commandant of the Marine Corps, the Atlantic and Pacific Fleets, and the Systems Commands.

INSIGHT

CIOs must personally lead change—effectively, passionately, and with an understanding of the stress that change brings to those in the midst of it. Leadership and commitment are often the only things that will stem the tide of discouragement when those around you are failing to deal effectively with change.

Following the Knowledge Superiority leadership dialogue at the Naval Academy, KM champions were rapidly emerging across the Department. An early champion and leader in KM implementation was the Commander of the Pacific Fleet, a four-star admiral out on the front lines. As he began to demonstrate and communicate his KM successes, other leaders recognized the potential value of KM to their organizations. A KM leadership network quickly spread across the Enterprise.

Quotes from early leaders and champions were shared through presentations; video cameos of Military and Civilian leaders were captured for wide distribution via VHS tapes, the Internet, and computer disks; and the language and ideas of the IM/IT Strategic Plan began to creep into everyday conversations and actions.

4. FACILITATE A COMMON UNDERSTANDING

So often we, as human beings, leap forward with little thought for the consequences. While a shared vision certainly helps define the direction we are leaping, for a large, complex organization, it is imperative to develop a shared understanding of the reasons behind the movement toward that vision to ensure a connectedness of choices. This connectedness of choices means that decisions made at all levels of the organization, while different, are made based on a clear vision of the future, and made in a cohesive fashion based on an understanding of why that future is desirable and the role that the decisions play with respect to immediate objectives in support of the shared vision.

Words and visuals are the tools of the trade for facilitating common understanding. Early DON models addressed those areas needing the greatest clarity, beginning with understanding the relationships among IT, IM, and KM (see Figure 9-3).

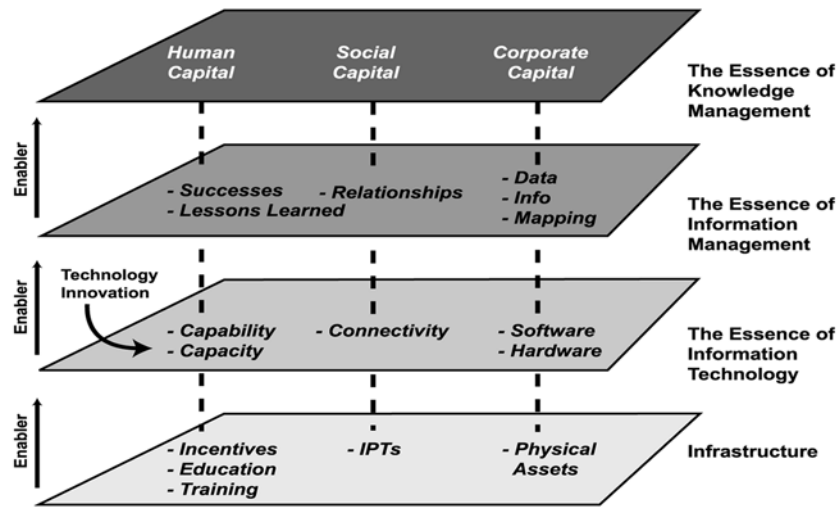


Figure 9-3—IT, IM, and KM collectively support the infrastructure and specifically, the decision-maker.

The message associated with this visual begins by reemphasizing that the role of IT is to support the infrastructure; that IT in and of itself exists to facilitate the management of information; and that the management of information is in support of decision-makers—people. KM cannot be effective without IM, which must be supported by good IT, which is embedded in the infrastructure. Additionally, KM, IM, IT, and the infrastructure all have elements of Human Capital, Social Capital, and Corporate Capital (see Section 5.2 for further discussion on these capitals). For example, the social element of KM is the interaction of people across networks built on relationships; the social element of IM is relationships among data and information; and the social element of IT is connectivity (through hardware and software).

An early model began the journey to move the bureaucratically-imbedded concept of “knowledge is power” to the emerging concept of “knowledge shared is power squared.” The Knowledge Life Cycle model, shown in Figure 9-4, generated dialogue on the relationship among data, information and knowledge; the reality of information decay (information has the potential to become less important over time); and the effects as knowledge spreads across the competitive base.

While the intent of this model was to engage response—thereby generating focused thought—there were common themes. For example, as knowledge is shared across organizations, it becomes more widely used. On the negative side this means that competitors now have the same opportunities causing erosion of the value of these ideas; on the positive side, since ideas generate ideas, everyone has a greater opportunity to build new knowledge innovation and implementation in the innovation life cycle characterized in Figure 9-1. What becomes of paramount importance is how those ideas are used. Another common dialogue that emerged focused on creativity. Since all people are creative, and everyone in today’s developed world has access to an almost exponentially increasing amount of information, then it is likely that any given creative idea will emerge in more than one place.

Once again, what is paramount in a competitive market is continuous learning (creation of new ideas) and the ability to effectively act on those ideas.

In the case of Critical Infrastructure Protection (CIP), after a basic effort to define CIP and the “infrastructures” this effort seeks to protect, Figure 9-5 has proven useful in establishing a common understanding of the activities which would form the foundation of an effective CIP effort.

We have defined DON CIP as an Enterprise-wide partnership of organizational entities that are essential for the Department to achieve effective protection of critical infrastructures; and defined critical infrastructures to include systems and assets—physical and cyber, DON-owned, and non DON-owned, such as state/local and commercially owned infrastructures—that enable the DON to accomplish its warfighting mission and core business processes.

Figure 9-5 reflects the six phases for CIP (also referred to as the CIP event cycle). The six Phases are: Analysis and Assessment, Remediation, Indications and Warnings (I&W), Mitigation, Response, and Reconstitution. Analysis and Assessment involves the set of activities required to identify which infrastructure assets are most critical to Naval warfighters and to assess their vulnerability to loss. Remediation includes employing risk management techniques to remove or lessen identified vulnerabilities. This translates not only to fixing identified vulnerabilities, but ensuring appropriate planning and risk mitigation efforts are in place to assure Navy and Marine Corps mission objectives during a critical loss. I&W represents the need to develop a coordinated (physical and cyber) indications and warning capability against acts of terrorism, natural disaster, or error.

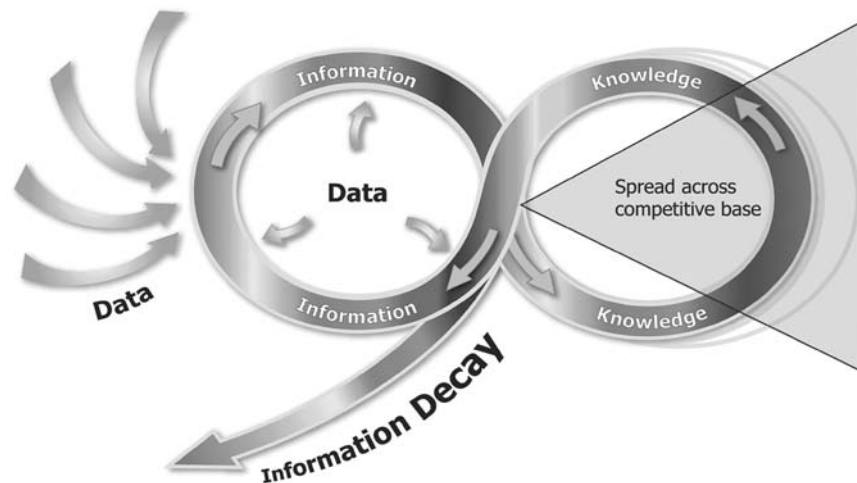


Figure 9-4—The Knowledge Life Cycle model is intended to generate thinking about the relationship among data, information, and knowledge; the reality of information decay; and the effects as knowledge spreads across the competitive base.

The last three phases of CIP—Mitigation, Response, and Reconstitution—are post event activities which represent the actual ability to execute risk mitigation strategies (contingency plans) and continuity of operations plans to continue to support the mission in the event of the actual loss of a critical infrastructure asset, and to reconstitute (replace or rebuild) that infrastructure as appropriate.

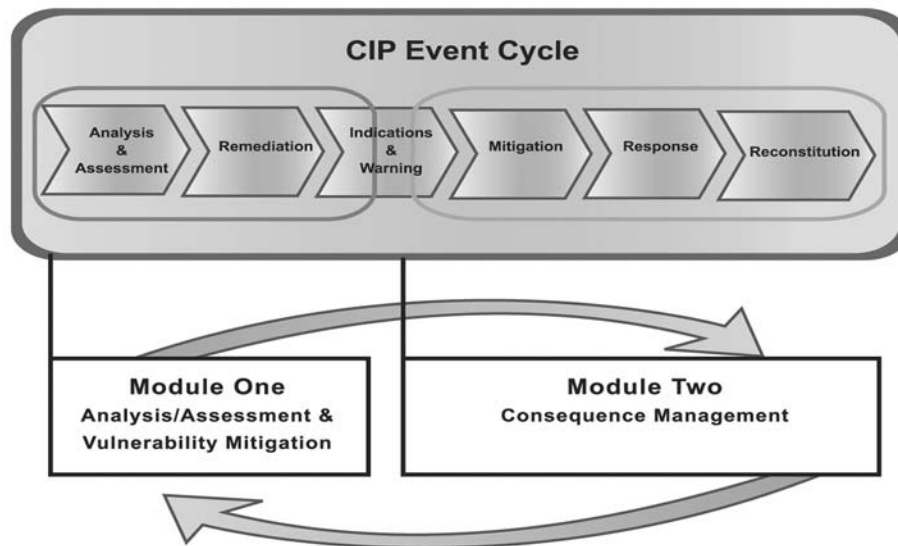


Figure 9-5—The six phases for Critical Infrastructure Protection are Analysis and Assessment, Remediation, Indications and Warning, Mitigation, Response, and Reconstitution.

5. SET LIMITS

All of the models discussed above limit the field of the possible in order to focus on a concept, facilitate a deeper understanding of that concept, and provide a mechanism for communicating that concept. We also set limits (provide focus) through developing and refining descriptions and definitions.

An early effort to set limits to encourage new opportunity was development of Enterprise-wide architecture and standards for IT, which documented the current and desired relationships between business/warfighting processes and the supporting IT infrastructure. The architecture was built on the Department of Defense Architecture Framework recognizing the operational, systems, and technical views (see Chapter 4 for further discussion on the DON architecture). Using an Integrated Product Team approach, DON CIO led development of Information Technology Standards Guidance and the Information Technology Infrastructure Architecture. These two important elements toward developing an Enterprise architecture provided limits in support of Enterprise interoperability, facilitating the sharing and creation of new ideas.

With the emergence of eBusiness (eB) concepts, the DON clearly built relationships between KM and eBusiness to harness the synergy between these two management focus areas. An article published in the Fall 2000 DON IM/IT magazine, co-authored by the CIO and the Chief Knowledge Officer, limited—or focused—KM and eB through the expansion and comparison of definitions. The focus of KM on intellectual capital—with KM viewed as a process for optimizing the effective application of intellectual capital to achieve organizational objectives—means people; while eB is the interchange and processing of information via electronic techniques for accomplishing transactions based upon the application of commercial standards and practices. These definitions reflected a common focus viewed through different lenses. Continuing the analogy, both eB and KM bring with them a focus on processes. KM provides a methodology for creating processes within the organization to promote knowledge creation and sharing—processes that build on total quality and business process reengineering concepts. In like manner, an integral part of implementing eB is the application of business process improvement or reengineering to streamline business processes prior to the incorporation of technologies facilitating the electronic exchange of business information.

KM, implemented by and at the organizational level, and supporting empowerment and responsibility at the individual level, focuses on understanding the knowledge needs of an organization and the sharing and creation of knowledge through communities and Web-enabled collaboration—connecting people. The knowledge systems supporting these communities, based on interoperability concepts to ensure Enterprise-wide sharing, build on IM, taking into account the human factor. While both KM and eB are in the business of information exchange, the KM focus is specifically on the knowledge sharing aspect of this exchange. This focusing of KM and eB—or setting of limits—provided a rich fabric for the two strategic efforts to complement each other and for the organization to recognize that both efforts offered opportunities for long-term success.

6. SHARE NEW IDEAS, WORDS, AND BEHAVIORS

Thinking in new ways demands new words (or putting old words together in new ways) to communicate that thinking; and those new words (or combinations of old words) drive new behaviors. In like manner, new behaviors drive new thinking and new words. As early as 1784 Hugh Blair identified a clear, close alliance between thought and language, “Thought and Language act and react upon each other mutually.” Later theorists such as Brown, Black, Bloomfield, Skinner, and Quine regarded language as a major form of behavior, a significant entity in its own right. In a writing text published in 1983, Emig contended that language is a powerful, if not unique, way of constructing reality and acting on the world (Emig, 1983). While the theoretical tapestry that builds relationships among thinking, language, and actions is varied and inconclusive, it is clear that there is a relationship, and that effective use of words, and understanding the concepts those words represent, have the potential to affect thoughts and behaviors

As an example, take the concepts of clustering and clumping. While these words have long been a part of Webster’s collection, the way they are used in IM and KM drives a necessary change in behavior. Clustering and clumping define different ways to access data and

information. Clustering is how data and information are usually organized, bringing together those things that are similar or related. This way of organizing is driven by the data and information itself. Clumping is driven by the decisions that need to be made. At the Enterprise level, those authoritative data fields that are needed for decision-making are identified and connected to provide real-time input to emerging decision-making requirements. In a system, that means linking secondary data and information needed by the individual who will use the primary information for decision-making. For example, if a Sailor has repeated failure of an engine part that is only periodically used, not only is it important to know how to fix it, but it would save considerable time, effort, and dollars if he had the knowledge that the engine was going to be replaced during the next port visit. There are often pieces of information that, if known, would change the decisions we make on a daily basis.

A second concept, which is included on the DON Knowledge Management Framework (see Figure 5.2-2), under culture, is verication. Verication is the process of consulting a trusted ally. When you do not have explicit evidence to verify the correctness of a decision, or you question the explicit evidence you do have because of your “gut” feeling, you can vericate the decision. This means going to a recognized expert with whom you have a relationship—a trusted ally—to get their opinion, i.e., grounding your decision through implicit knowledge. How many times have you personally picked up the phone or sent an e-mail to someone you know could help you answer a question? This process of verication is consistently used by both individuals and organizations in the decision-making process.

An important concept here is, of course, the sharing of those new ideas, words, and behaviors. An aggressive, comprehensive communications strategy, both internal and external, is essential to ensure the connectedness of choices discussed earlier. Internal successes and external validation provide strong explicit evidence in support of the business case. The use of teams and communities—an important KM strategy—helps facilitate the flow of information and knowledge across the organization. As the DON recognized the value and opportunity offered by this new approach to communicating, sharing, and innovation, communities have emerged across the DON Enterprise.

7. IDENTIFY THE STRATEGIC APPROACH

At the Secretariat level, DON implementation of the IM/IT Strategic Plan is built on a systems model that addresses decision-making capability at the individual, organizational, and Enterprise levels. The continued surge of IT investments over the past few years has significantly increased the amount of data and information DON decision-makers have available, thereby increasing the complexity of decision-making. As this complexity increases, DON has invested more and more in IT to help solve the problem, thereby further increasing the amount of data and information available to decision-makers, and increasing decision-making complexity. This reinforcing cycle continues. Applying the Systems Thinking approach coming out of the Massachusetts Institute of Technology’s work on learning organizations, the DON began creating balancing loops to break this reinforcing cycle. While recognizing the need for the Department to continue developing and embracing new

IT capabilities, these balancing loops address the systemic issues of how that technology is used at the individual, organizational, and Enterprise levels.

At the individual level, as decision-making complexity increases, new cognitive skills are needed that will allow each of us to do more with our innate capabilities. Systems Thinking skills are one way to achieve this. Systems Thinking is a diagnostic methodology for understanding and assessing cause-and-effect relationships and identifying leverage points. It enables a clearer perception of the full patterns of change and the structure of systems to better comprehend their behavior and make appropriate responses. As the individual learns and applies systems thinking, individual decision-making capability increases by focusing on leverage points, thereby reducing decision-making complexity and breaking the cycle described above. The DON has developed a Systems Thinking virtual training package to facilitate learning. This learning tool is available to every Sailor, Marine, and DON Civilian via CD or the Chief of Naval Education and Training portal.

At the organizational level, increased decision-making complexity drives the need for information and knowledge systems. As new and improved processes are put into place, bringing tacit knowledge into the explicit realm and connecting critical data for decision-makers, decision-making capability improves, thereby reducing decision-making complexity and helping to further break the cycle defined above. The DON developed a knowledge-centric organization (KCO) toolkit to facilitate KM implementation at the organizational level. KCOs are able to leverage their personnel and critical technology assets jointly, creating knowledge and then communicating it to the right person at the right time to solve problems. Ultimately, KM strategies facilitate collaborative information sharing that optimizes strategic and tactical decision-making, resulting in more effective action.

A good example of collaboration at sea is the Stennis Battle Group project. A Battle Group is an aircraft carrier accompanied by a group of escort and support vessels. Collaborating at sea is difficult. Limited bandwidth impairs the ability to connect a large group of worldwide users to a massive amount of information with sufficient speed and accuracy. Historically, Battle Groups have struggled with the need to capture, archive, and later access key data and unique processes associated with repetitive operational deployments. It has been difficult to transfer lessons learned from one Battle Group exercise to another, and almost impossible to transfer and leverage knowledge efficiently. The Stennis Battle Group project developed the capability for rapid and flexible collaboration, planning, and execution of all Carrier Battle Group operations. The use of commercial off-the-shelf products ensured industry standards and leveraged industry investment, avoiding the life cycle costs of owning the equipment. The use of a common taxonomy developed an instantaneous, context-oriented communications capability including audio, video, and applications sharing. The bottom line is that the Project team was able to establish a classified Battle Group collaboration environment as a repository of the current tactical picture, forming the basis for an expansive implementation of KM that included development of the knowledge-centric concept of operations. Because of its success, the Stennis Battle Group project is being emulated by other Battle Groups in both the Atlantic and Pacific Fleets.

Implementation at the Enterprise level must be discussed in terms of connectivity and flow. While connectivity certainly relies on the hardware and software infrastructure provided by IT (see the discussion of the Navy Marine Corps Intranet (NMCI) in Section 4.5), it goes beyond the wires and bytes to connecting people and facilitating understanding. With Enterprise connectivity comes a massive proliferation in the quantity of electronically available information, creating an information overload on network systems that makes it very difficult for users to find necessary information in the time they have available. Information is commonly organized within an Enterprise's repositories with classification systems designed within a conceptual framework. These frameworks allow information to be consistently classified to make it easier for users to know where to look for various types of documents and records. This framework is translated into a hierarchy of descriptive categories that form the taxonomic schema used to control the classification process. Integrated with data management and interoperability meta-data standards, the DON developed a framework for its Enterprise taxonomy that builds on lessons learned from organizational content management projects and technology tool performance tests to incorporate sufficient flexibility and adaptability, thereby allowing all users to operate as efficiently as possible (see Section 5.5 "Knowledge Taxonomy").

8. DEVELOP THE INFRASTRUCTURE

As technology advances, a seamless infrastructure is essential to facilitate the collaboration and free flow of information that enable effective decision-making. A first step to achieving this infrastructure was development of NMCI. The overarching importance of IM and KM to improve decision-making led DON to conclude that managing information, and creating and sharing knowledge—rather than owning the necessary technology—were the primary IM/IT business of the Department. If the IT infrastructure used did not need to be owned, it could be treated as a service, much like gas or electric service.

In October 2000, after a year-long exploration of the feasibility of this approach, the DON awarded a seat management contract to Electronic Data Systems to provide an all-encompassing information/communications technology solution. This solution, the NMCI, gives Civilians, Sailors, and Marines access to the rich intellectual resources that extend throughout the Naval Enterprise. Replacing the Navy's numerous shore-based networks, NMCI as a technology infrastructure provides data, video, and voice services to Navy and Marine Corps personnel, to ensure access, interoperability, and security for information and communications needs. Coupled with the Navy's shipboard system and the Marines' tactical network, the intranet gives Sailors and Marines forward-deployed around the world direct access to the network of people, information, and knowledge available in government, industry, and academia. NMCI makes connectivity transparent, with forward-deployed forces having immediate access to the best resources available—a "reach-back" capability that provides the knowledge they need to make critical mission decisions.

With the advances in technology, such as NMCI, that the DON is embracing, it was imperative that the Department have a workforce able to cope with the new technologies. In the summer of 2001, the DON issued a call for action for both Civilian and Military workforce planning to ensure the DON can meet its future IM/IT missions. The report

presents the results of an IM/IT workforce gap analysis conducted at the DON level which addresses: (1) the estimated number of Civilian workers required in FY2005; (2) the competencies necessary to achieve projected IM/IT missions; and (3) strategies and initiatives to help the DON attract new personnel and sustain the capabilities to accomplish its missions. A DON Workforce Strategic Plan for 2001–2006 requires Department CIOs to develop strategies and specific plans for hiring, training, and professional development, with the goal to promote IM/IT and KM competencies throughout the workforce. Thoughtful, visionary, and forward-thinking, this plan lays the foundation for positive organizational transformation, with the potential to benefit the entire DON.

A DON *Civilian Career Path Guide* (CPG) was developed to provide individual guidance to employees in meeting the continuing challenges of technological change. The CPG offers guidance to Knowledge Management practitioners, establishing KM capabilities for the DON to employ in pursuit of becoming a knowledge centric organization. The KM career area includes the following roles: Chief Knowledge Officer, Knowledge Manager, Knowledge Systems Engineer, Knowledge Process Manager (for larger organizations broken down into the three roles of Knowledge Transfer Engineer, Knowledge Research Engineer and Knowledge Life Cycle Engineer), Knowledge Community Leader, Intellectual Capital Manager, Performance Measurement Engineer, Knowledge Assurance Manager, and Knowledge Assistant. Explication of these roles and related learning objectives are available from the DON CIO. The CPG also addresses the issue of outsourcing those jobs better suited to the private sector.

A Workforce virtual resource was developed in the spring of 2001 that includes the DON *Civilian Career Path Guide for Management of Technology, Information and Knowledge* and an interactive Career Planning Tool that helps the Civilian IM/IT and KM workforce assess their current and required competencies, and generates a Career Progression Plan to attain competencies needed for future job assignments based on individual, long-term goals. The virtual resource includes the *Workforce Strategic Plan*, *Inherently Governmental Guidance*, and *Call for Action and Gap Analysis* discussed above.

9. MEASURE AND INCENTIVIZE

In a survey conducted in 2000, a DON organization implementing a KM pilot (approximately 250 people) identified the most important factors in successful KM implementation in this relative order: culture (29 percent), processes (21 percent), metrics (19 percent), content (17 percent), leadership (10 percent), and technology (4 percent). What is fascinating, and a product of the DON culture as well as many organizations in industry, is that metrics (how success is measured and communicated) appeared more important than content (that which is in the system itself). The bottom line is that metrics are an important aspect of the DON culture.

In August 2001 the DON published a *Metrics Guide for Knowledge Management Initiatives*. The guide focuses on three types of specific measures to monitor KM initiatives from different perspectives: outcome metrics (concerning the overall organization and measuring large-scale characteristics such as increased productivity or revenue for the Enterprise); output metrics (measuring project level characteristics such as the effectiveness

of lessons learned information to capturing new business); and system metrics (monitoring the usefulness and responsiveness of the supporting technology tools). The guide includes a discussion of qualitative and quantitative measures, a KM maturity model, and case studies.

In October 2001 the DON published the *Guide for Developing and Using IT Performance Measurements*. This guide provides an outcome-oriented method for measuring the impact of IT investments on the organization's mission, goals, and objectives. To achieve this end, the guide recommends the use of Kaplan and Norton's Balanced Scorecard, modified for the Federal Government. The guide takes users through the iterative process for developing and managing IT performance measures. The process begins with the definition of the investment and involves constant refinement and management throughout the life cycle of the asset.

The Balanced Scorecard, using the process described in the *Guide for Developing and Using IT Performance Measurements* provides a model for ensuring that the investment will be continually evaluated from the perspective of the customer and the stakeholder, and will also be continually evaluated from the financial perspective. The model helps ensure that objectives and measures are evaluated related to the perspectives of learning and growth and internal processes within the organization. From this standpoint, it is a far better method of measuring performance as compared to traditional cost and performance measures. The real value to the DON is its strength in increasing the probability that IT investments lead to improved mission performance and information superiority.

As IM/IT successes began to emerge throughout the DON, the Secretary of the Navy established awards to recognize those teams which were increasing effectiveness and achieving efficiencies through knowledge sharing. These included awards ranging from the "Outstanding Knowledge Expert System" presented to Virtual Naval Hospital for its delivery of expert medical information to the "Operationalizing KM Concepts" award presented to the Naval War College Global War Game KM/IT Team for implementing processes to exploit and distribute information and share knowledge that dramatically improved decision-making. Clearly, IT, IM, and KM are making strides toward *putting information to work for our people*.

10. PROVIDE TOOLS

Buckminster Fuller once said that if you want someone to change, give them a tool. The DON approach to change recognizes the truth of this statement. As guidance and policy are issued, tools that provide approaches to and resources for accomplishing that guidance and policy are distributed. These toolkits are published on CDs and made freely available to all government, academia, and industry support organizations, with the understanding that change in a complex organization must be validated externally while driven internally. Forward-thinking and forward-movement in other government organizations, and by our industry partners, supports and promotes DON forward-thinking.

These virtual resources, which have been distributed by the tens of thousands, fall broadly in the areas of guidance tools, learning tools, process tools, and communications

tools. Virtual tools in the area of guidance cover Capital Resource Planning and Investment Practices, Architecture and Standards, Critical Infrastructure Protection, and Workforce. Virtual learning tools include a course on Systems Thinking, and an Information Literacy resource. Virtual process tools support becoming a Knowledge Centric Organization and Business Process Reengineering. Virtual communications tools include a resource on Privacy and a compendium of eB and KM systems (extending the sharing begun at each Knowledge Fair worldwide).

11. PROMOTE LEARNING

You cannot change without learning, nor once you have changed can you continue to function and be of value in a changing environment without continuous learning. Though this important concept emerged a dozen years ago in the Total Quality environment, we're just beginning to realize the importance of it, and putting systems in place to help facilitate learning in a virtual world.

In 1999 the DON issued its first Continuous Learning Guidance for the core IM/IT workforce. This guidance placed increased responsibility on employees to remain current by taking advantage of new ways of learning. Distributed learning technologies, experiential learning, and other nontraditional approaches to education and training were rapidly supplementing the traditional classroom student/instructor approach. With these new approaches, the DON valued the ability of learners to take responsibility for and direct their own learning and development in a variety of ways, and on a continual basis, throughout their careers. The guidance set the expectation that all Civilian and Military IM/IT core workforce professionals participate in 80 hours of continuous learning activities each year to augment the minimum competencies established in their career fields and required for specific workforce assignments. The core IM/IT workforce was defined as those personnel who are focused on Military and Civilian IM/IT careers. This groundbreaking document was a precursor to the first IM/IT Workforce Strategic Plan, which widened and broadened the definition of the IM/IT workforce beyond the core mentioned above. The bottom line is that every person who uses IM/IT—and that's nearly everyone in the DON, or should be—needs to become a continuous learner to move the DON toward becoming a learning organization.

Recognizing the importance of being a learning organization to become knowledge-centric, in the winter of 2001 the DON developed an Organizational Learning toolkit. The toolkit focuses on learning in a virtual world, defining learning, and exploring aspects of virtual learning and its relationships with KM, intellectual capital, and communities and teams. It includes assessing individual and organizational readiness for virtual learning, a model for developing effective virtual learning courses, an information technology support matrix, and a compendium of virtual learning courses available across the Department. The toolkit paves the way for building a larger understanding of the value and importance of virtual learning to the future success of the defense of our nation.

12. VISION AN EVEN GREATER FUTURE

The place from which we currently act and respond, our point of reference, is reflective of the bureaucratic model upon which our organizational structures were grounded. As a groundswell of change is created, the Department's point of reference also changes. Ensuring continuous improvement and accelerating reengineering, new ideas and new thoughts need to come into focus and enlarge the future vision to ensure sustainable performance advantage. This, of course, is the role played by new management movements, as organizations in the Western world moved through Total Quality Management and Business Process Reengineering, and are now implementing eBusiness and Knowledge Management. What is critical for future success is an organization's ability to take the best of each new focus area, determine fit, and integrate the best from each into the organization in a way that makes sense.

In the complex world in which we live, there is no lack of new management approaches, and assuredly each approach offers potential value. What is difficult is to achieve the balance among recognizing and sustaining that which is good in an organization, embedding that which has been determined valuable and is currently being implemented, and embracing the value offered by new ideas. What is that balance? What are the potential gains and losses from this approach? How do we facilitate the gains and mitigate the losses? Finally, since a complex organization cannot be controlled in the classical meaning of the term—nor should it be—how do we ensure that value, as it emerges, is shared across the organization?

This dilemma of balance extends through every aspect of an organization. A visible example is the insertion of new information technology such as wireless. At what point does the organization wishing to succeed in the future global world embrace wireless technology? How fast should this transition move? What mindsets and strategies (such as moving the security focus from technology to information) need to be changed?

In many cases, a bar must be set, even if it is a somewhat arbitrary bar. When Larry Ellison, the CEO of Oracle, announced that he would take one billion dollars out of his company's overhead expenses within a year, he set a target. A target or goal (limits), provided by an organizational leader, even a seemingly arbitrary goal, can often be the stimulus that encourages an organization to begin the journey of change.

In the film, *Indiana Jones and the Last Crusade*, the intrepid Indiana finds himself literally on the precipice in his search for the Holy Grail. Even when confronted with the realization that he must get across the chasm that spreads before him, he is still temporarily immobilized by the seemingly insurmountable nature of the challenge before him. As he stands on the edge, he recalls his father's words—that the successful completion of his quest will require a "leap of faith." Summoning his courage, he slowly takes that first step, and as he feels like he is about to fall into the abyss, his foot lands securely on a pathway across the chasm...a pathway hidden from his sight by a trick of light and color. With his new found change of perspective, it no longer looks like a "leap" at all, but rather a natural path to his goal.

Implementing change often requires a “leap of faith.” Through encouragement, forward-thinking policies, tools, and targets, effective CIOs can help even the most hide-bound organizations successfully adopt change. And in the end, the act of personally leading change is required from everyone, at every level of the organization.

CONCLUDING THOUGHTS

The Department of the Navy’s approach to creating an Enterprise intranet—treating the information technology infrastructure as a service—provided the opportunity for the Department to focus on managing information and knowledge, facilitating the decision-maker’s use of the information enabled by information technology. Thus, KM has been effectively married to an aggressive IM/IT program, providing the value that links effective information technology and information management to the people who use that information. This focus on people has been holistic, ranging from the creation of theory and building of shared understanding to the development of infrastructure to support individual and organizational learning.

Enterprise-level leadership ranges from promulgating guidance and policy, to providing tools, to rewarding success, and facilitating cultural change. While each of the steps discussed in this Chapter builds on the underlying theme of “cultural change” and offers specific direction and actions, the importance of successfully addressing cultural change cannot be overemphasized. The single most pervasive theme in all initiatives undertaken by a CIO is change. The ability to effectively lead change is paramount. While the insertion of new technology is often a key enabler, the work associated with the technology insertion is only a small part of the effort required to successfully implement IM/IT initiatives. The large percentage of a CIO’s effort must be focused on addressing cultural change.

As with other organizations, the Department of the Navy is moving forward at a fast pace, with a vision and strategy, on a path not limited by preconceived notions. The path is being forged by thousands of dedicated professionals, working individually and collectively. Effectively, the complex DON change strategy is encouraging the natural progression from a focus on information technology to a focus on how information is managed and used by decision-makers, *putting information to work for our people*.

The Future and the CIO

We live in an uncertain world. On September 11, 2001, terrorists attacked the United States of America. The Pentagon was a primary target. The Navy Command Center and Budget Office were at ground zero. With 70 percent of the Navy's space inside the Pentagon seriously damaged, immediate steps had to be taken to relocate the Navy staff in temporary spaces in the National Capital Region, and to rebuild its classified and unclassified networks.

The Navy Marine Corps Intranet (NMCI) contract served as the prime vehicle to undertake this critical effort. On Wednesday, September 12, the prime contractor, EDS, was contacted and asked to set up a temporary Naval Command Center capability in the Marine Corps Command Center. By Wednesday evening EDS was provided an estimate of the number of NMCI seats the Department would need to reconstruct its lost capabilities. EDS and the Information Strike Force went to work. They put out a call for all available cablers, network engineers, and setup specialists up and down the mid-Atlantic region to descend on Washington, DC. Thursday morning, nine 18 wheelers left EDS's staging facility in St. Louis, MO filled with 860 portables, 335 desk side computers, and enough CAT-5 cabling, fiber optic backbone cables to outfit five floors of office space. A separate 18 wheeler left Cisco headquarters in San Jose, CA with all of the routers and switches necessary for completion of the outfitting. Friday morning the 18 wheelers arrived in Washington, DC, and distributing and connecting began.

The Command Center was operational by midnight on Friday. All critical systems were operational and information recovery was complete by Sunday. Crisis relocation and reconstruction efforts were accomplished by Wednesday, September 19. Using the NMCI as the single point of implementation allowed the Department to rapidly recreate all of the capabilities lost in the attack on the Pentagon.

This fluid collaboration between government and industry in response to the events of September 11 occurred throughout the United States and, indeed, throughout the world. In a speech to the National Academy of Public Administration on November 16, 2001, the Honorable David M. Walker, Comptroller General of the United States, said:

It's truly amazing and inspiring how Americans can pull together without regard to turf considerations and other artificial boundaries to get the job done in the event of a crisis. While this is impressive, we must begin to be able to work in this fashion in the normal course rather than in a crisis. This will be tough, but it is essential in order to maximize the government's performance and assure positive outcomes.

So, after the shock and surprise of September 11, what does the future hold and what can be done to ensure the future efficiency and effectiveness of our government through Information Management/Information Technology (IM/IT)? We are all too familiar with the accelerating pace of technology, communication, and transaction rates. Social and

economic changes are somewhat slower, but they are there nonetheless, and not easy to predict. The continuing world political turbulence, coupled with the rise of weapons of mass destruction, makes it difficult to rationally predict future scenarios. However, if we look for generic characteristics within our current and future environment, we will be better able to anticipate the IM/IT needs of our government. These high level characteristics can best be recognized as **accelerating rate of change, increasing uncertainty, and growing complexity.**

INSIGHT

Knowledge itself has no inherent goodness or badness. On September 11 our adversaries successfully managed knowledge to achieve their objectives. What this realization means is that as we gain knowledge and act upon it, we have the responsibility to ensure the value of those actions both in terms of our Naval mission and in terms of the greater good for humanity at large.

While the increasing rate of change has been a characteristic of history since the Renaissance, it can now be described as exponential. Science and technology build upon themselves. The more we understand, the more we learn and create new ideas, inventions, and applications. Since World War II, with the creation of computers and the digital world, the rate of data and information flow has been exploding and there is no end in sight. The Internet, virtual broadband, video streams, cell phones, satellite systems, Global Positioning Systems (GPS), etc. all inundate us with data, information, and sometimes knowledge. This brings about an increasing pace of transactions such as the instant movement of money, and rapid communications through multiple, instant, visual interactions supported by knowledge repositories. All this places us in a dizzying, hectic world—one that everyone will have trouble keeping up with, but within which everyone must live and perform well. The result is likely to be a world in which problems, issues, events, opportunities, and disasters will come fast and furious from all directions.

The second major characteristic of the future is the difficulty of predicting or even anticipating near-term events. Historically, it has been easier to anticipate the near-term environment and much more difficult to estimate what will happen in the future. While in theory this may still be true, even near-term environments hold great surprises, thereby making near-term decisions challenging. When this uncertainty is coupled with the accelerating rate of change, problems become compounded.

The third characteristic is the growth in complexity of the environment. Complexity results from a large number of elements, or events, with many relationships among them. Complex systems are difficult to understand and their behavior hard to anticipate. Yet effective decisions and actions depend upon our ability to understand and anticipate the results of those decisions and actions. As technological, social, economic, and political systems become more complicated, this problem of inadequate knowledge to make and implement good decisions will become increasingly critical for the effective performance of the government.

In summary, the pace of change will continue to rise, uncertainty will be greater and more widespread, and many parts of the world will be made up of more and more complex systems. Given this, what can CIOs do now—within their IM/IT and corollary responsibilities—to help their agencies/organizations sustain high performance? There are three major focus areas that help move us toward the future: interoperability, ubiquity, and knowing.

MOVING TOWARD INTEROPERABILITY

Interoperability is built on connectivity. It connotes the flow of information (and ideas) across organizational and geographic boundaries, and the flow of information (and ideas) across time, bringing the lessons learned from the past and the vision of the future to the actionable present. Networks and relationships provide the framework for interoperability, bringing people together virtually to share information and knowledge. Interoperability enables organizational flexibility and robustness through rapid communication and common understanding of the organization's shared vision.

More and more we live in a connected world, and the reality of September 11 is accelerating our recognition of the need to fully develop and use that connectivity. For the Department of the Navy, the Navy Marine Corps Intranet is the foundation of that connectivity, and will become a part of the larger Department of Defense network, which in the future will become part of a larger government-wide network in support of all citizens, enabling eGovernment.

eGovernment is not a new concept, but the challenges presented by today's changing environment, discussed above, are new and pervasive. As we entered the new Millennium, the Federal Government launched the FirstGov.gov portal, providing one-stop shopping for government information. This is only the beginning. As Enterprise portals that allow for self-service transactions become the norm, Federal employees and the general population will expect more and more opportunities to leverage technology to improve their quality of life and enhance personal productivity. Walls between government-to-government and citizen-to-government transactions will be broken down. It will become the norm to move seamlessly over the course of the day from business transactions to applications that provide for professional growth or personal business. Authentication solutions will recognize that one individual can have identity changes hour by hour, gaining access to their network in the office, gaining access to the day care center to pick up their children, authenticating themselves at an airport terminal, or conducting a secure transaction from their home computer in the evening.

The debate over the virtues of a national identification card will continue to rage. Proponents will tout the security advantages of assured identification. Critics will continue to lament the potential loss of civil liberties. As an alternative to a single national identification card, the move toward standards-based interoperable solutions may pave the way for a national "interoperability card" system—a single card or collection of cards that would allow citizens to move through the various "roles" that they fill over the course of a day. With the maturity of public key infrastructure (PKI), cryptographic-based smart cards, biometrics, and contactless (proximity) card capabilities, more and more businesses and

Federal agencies will follow the path already being implemented by the Department of the Navy to use the power of digital certificates to positively identify individuals and allow them access to the transactions they need to conduct. Cross certification of PKI certificate authorities, standard formats for digital certificates and common smart card platforms and operating systems will allow this “web of trust” to continue to grow, expanding the opportunity for Navy and Marine Corps employees to use the digital credentials on their smart cards for transactions away from the office.

In a logical extension of the authentication technologies contained on the Uniformed Services Identification Card, state governments could also pursue interoperable smart card solutions, adding smart technologies to drivers’ licenses and state identification cards. As the population of citizens with smart card, PKI, and biometric technology continues to grow, the business case will be made for commercial firms to modify point of sale and access devices to recognize these capabilities. In the future, this single national interoperability card system could provide the means to ensure secure transactions over the Internet and provide greater certainty of individual identity at airports and office buildings. Strong authentication technologies will also enhance user experience, as systems and Web sites are instantly customized to best accommodate the needs of the authenticated individual. Personal security will be enhanced, fraud will be reduced, and opportunities to increase the flow of knowledge will flourish with the implementation of a national interoperability card solution.

The emergence of Communities of Practice (CoPs) are facilitating collaboration and interoperability, promoting the sharing of lessons learned and the exchange and creation of new ideas. CoPs are one of the new organizational forms of the Millennium. They are built on the tradition of professionals joining together to share skills and resources, and are vibrant learning centers and rich marketplaces for learning and knowledge sharing. New communities quickly formed in strategic areas following the events of September 11, and have been rapidly spreading across the government. The Department of the Navy was an early implementer of communities, and this powerful form of collaboration and learning is changing the flow of information (and the sharing of knowledge) at organizational and Enterprise levels. The sharing of knowledge improves the understanding of complex events and systems, thereby aiding more effective decision-making. Such understanding also leads to improved anticipation of future events. DON will continue to champion this important transformational initiative.

MOVING TOWARD UBIQUITY

As people rely more and more on virtual resources, they create a continuing demand for connectivity, and availability, any time and any place. Ubiquity implies being, or seeming to be, everywhere at the same time; in this context it represents the omnipresence of information. Ubiquitous communication is part of the DON’s vision of the future. Availability of information to decision-makers when and where it is needed facilitates rapid decision-making that can respond to the speed of change, using information technology as an enabler for a mobile, global workforce.

While wireless technology is not new to the Department, what is new is the introduction of wireless technologies to the user. Wireless technologies in the hands of our Sailors, Marines, and Civilians are changing the way we work and learn. For example, with desktop computers, users were required to be physically located at a station to feed or consume information. Wireless allows us to bring the systems to where we work, whether in a conference room, on the flight line, or even on a bench while waiting for a shuttle.

There are dozens of new products coming onto the market or in development that will facilitate the availability of information at any place and time. Various research centers are developing systems that will educate the user about their surroundings as well as provide timely information under adverse environmental conditions. For example, a National Air and Space Administration Jet Propulsion Laboratory prototype of “wearable technology” can relay to the astronaut her vital signs, provide the spacecraft’s system status, and display manual excerpts through a liquid crystal display (LCD) eyepiece—all of this while communicating the astronaut’s actions to ground control. In the Military setting, soldiers can receive new navigational maps and blueprints through their LCD devices, and Military medics can instantly address health concerns of injured Marines by reading their biometric signs, and locating them with GPS location devices.

New collaboration aids will support interoperability around the globe. For example, researchers with the Office of the Future Project at the University of North Carolina Chapel Hill are working on blending holography, virtual reality, and conferencing to create meeting experiences in which the subjects are viewed as within the same place independent of their location. In another research project, subjects involved in the Cave Automatic Virtual Environment at the University of Illinois at Chicago are able to interact with dispersed virtual objects by wearing lightweight stereo glasses. The Indiana University Virtual Reality/Virtual Environment Labs, using CAVE and ImmersaDesk technologies, have enabled physicians to either tele-collaborate or view in person and interact with high quality three-dimensional MRI and CT scans. These virtual reality tools provide researchers and engineers with the ability to navigate complex virtual worlds and gain new vantage points and insights in analyzing complex visual imagery.

New technologies are also being exploited to accelerate learning. Various research centers, expanding upon the concept of transparent computer-user interfaces, are exploring how truly transparent systems could be ideal for training purposes. The Naval Postgraduate School in Monterey, CA is taking eLearning to new heights, building on traditional distance learning efforts in the field of information assurance to also provide students with a “virtual laboratory” in which to practice their newfound skills. Research on cultivating peak performance suggests that lucid dreaming may prove to be an effective training ground. Even more radical than lucid dreaming as a training ground is the research being conducted by the Artificial Life Team at British Telecommunications in Ipswich, England. Their reports discuss the development of a chip that would be implanted somewhere behind the eye and interface with the user’s neural network, creating a truly digitized environment.

Just as historically, the latest weapons technologies have been a determinant of success in warfare, in the future the latest and best IM/IT will significantly influence the outcome of conflicts. The Department of the Navy is committed to the insertion of new technologies to increase mission readiness and enhance organizational effectiveness and efficiency. In a complex world faced with asymmetric and intermittent threats, decision-makers demand timely, valid, and relevant information. Interoperability and ubiquity can ensure that information is available. What remains is the ability of the decision-maker to know what they need and how to use it.

MOVING TOWARD KNOWING

Sun Tzu, the early authority on warfare strategy, believed that the moral strength and intellectual faculty of humans were decisive in war, and if applied properly war could be waged with certain success. This intellectual faculty consists of a combination of past experience, intuition, judgment, common sense, and the ability to comprehend complex situations within the context of immediate goals and objectives. In short, to deal with rapidly changing, complex, non-linear, uncertain situations, one must be able to see beyond images, hear beyond words, and sense beyond appearances. This is a blending of the cognitive capabilities of observing and perceiving a situation, the cognitive processing that must occur to understand the external world and make maximum use of our intuition and experiences, and the faculty for creating deep knowledge and acting on that knowledge.

This construct of knowing can be elevated to the organizational level by using and combining the insights and experiences of individuals through dialogue and collaboration within teams, groups, and communities. Such efforts will significantly improve the quality of understanding and responsiveness of actions of the organization. It also greatly expands the scope of complex situations that can be handled through knowing because of the greater resources brought to bear—all of this significantly supported by interoperability and ubiquity.

Organizational knowing is an aspect of organizational intelligence, the capacity of an organization as a whole to gather information, innovate and generate knowledge, and to act effectively. This capacity is the foundation for effective response in a fast changing and complex world. Support capabilities of organizational knowing include organizational learning, knowledge-centricity, common values and language, coherent vision, openness of communications, effective collaboration, and the free flow of ideas and people.

The Industrial Age was founded on society's use of complex machines as labor saving elements to shift the burden from men (and animals), changing the underlying transaction costs, hence, economies of production. These machines themselves are combinations of simple machines that cleverly provided mechanical advantage. Mechanical advantage is the ratio of output force divided by input force. When it is greater than one, it increases the force that can be applied to a task, making hard jobs easier and jobs some thought impossible, possible.

The “mental advantage” offered through knowing is built on information as a source used by the mind to create understanding. The ratio of mental advantage is analogous to

that of mechanical advantage: mental advantage is the ratio of output knowledge to input information. The greatest challenge facing all CIO organizations over the next decade is achieving and sustaining this mental advantage.

Organizational knowing is the key. Success in this undertaking could be as profound as that seen in the Industrial Revolution when at its zenith. The ramifications imply that the underlying economies and productivity of our workforce would take a giant leap ahead. This effort demands our full attention and resource commitment.

WHAT DOES SUCCESS LOOK LIKE?

The following story provides a glimpse into our vision of the future. It describes the power of interoperability, ubiquitous information, and the use of teamwork to create knowledge and through knowing, increase our mental advantage.

Among the forward-deployed forces of the Navy are three units engaged in vital operations in the Arabian Gulf, the Adriatic Sea, and the Sea of Japan. Data mining is underway among ships that are oceans apart. The maintenance bot, an automated analysis agent, discovers a disquieting pattern of premature part failures. In-service engineering support team members at different locations are alerted to the nascent trend by an analysis software program, and connected through voice and video software. Each team member brings a wealth of experience and insight to bear. A 3D digital product-process model is called up from the original equipment manufacturer's factory server. Joining the team interaction, factory and government design engineers run a virtual system simulator using the ships' equipment data logs that have been accessed and downloaded from the ships at the blink of an eye—the biometric click of a mouse. The interplay of observations, ideas, experiences, and perceptive knowing by the team surfaces the potential cause of the emerging critical part failure, an unexpected nonlinear sensitivity to the higher than normal humidity levels, combined with a sneak electronic feedback path.

After a collaborative exchange among the engineering team members, an innovative, subtle design parameter change is made digitally and thousands of replications of the Web-based simulator are run to verify the completeness and robustness of the re-designed component solution. The program manager, vacationing in her secluded mountain cabin, is alerted to the last 30 minutes of work via an e-mail delivered to her personal mobile communication device tagged as urgent by the team members. She authenticates and connects to the Department of the Navy intranet portal and the team agrees that the best visualization option would be to download the simulation through the family's satellite dish onto the high performance Play Station 2™ visualization tool. There is no need to worry about eavesdropping, or theft of information, as all of the voice and data transmissions are encrypted.

All the design and production team members spread across 16 time zones, using tablets, personal digital assistants, or cell phones, are able to view the 3D simulation simultaneously and securely. Drawing on their common understanding of the situation, their mutually-agreed-upon desired results, and their ability to relate complex concepts, i.e., Knowing, the team settles on the design change. The collaborating suppliers enter the nec-

essary changes into their automated order fulfillment system which initiates priority one shipping, alerts packaging, and re-routes commercial trucking and air express companies' planned pick-up and delivery schedules. The new parts are fabricated, integrated, shipped, received, and installed before the old parts actually break, thereby averting the loss of critical fighting capability that would affect battlegroup readiness. The various financial and inventory transactions of the shippers, suppliers, integrators, manufacturer, and engineers, as well as the ships and Fleets, are automatically updated behind the scenes without wasteful intermediary transactions. The authoritative technical manuals and engineering drawings are revised, lessons learned are exchanged through communities of practice, and virtual training modules are developed and disseminated.

Our ships in the Arabian Gulf, Adriatic Sea and Sea of Japan steam ahead, continuing their uninterrupted operations, maintaining Naval readiness—and ensuring our National Security.

Acronym List

AAAV	Advanced Amphibious Assault Vehicle
AAP	Abbreviated Acquisition Program
ACAT	Acquisition Category
ACMC	Assistant Commandant of the Marine Corps
ACT	Acquisition Coordinating Team
ADA	Americans with Disabilities Act
Air Force CIO	Chief Information Officer, Department of the Air Force
AIS	Automated Information Systems
APQC	American Productivity and Quality Center
ARG	Amphibious Ready Group
Army CIO	Chief Information Officer, Department of the Army
ARO	Acquisition Reform Office
ASD (C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASN (FM&C)	Assistant Secretary of the Navy (Financial Management and Comptroller)
ASN (I&E)	Assistant Secretary of the Navy (Installations and Environment)
ASN (M&RA)	Assistant Secretary of the Navy (Manpower & Reserve Affairs)
ASN (RD&A)	Assistant Secretary of the Navy (Research, Development and Acquisition)
ASW	Anti-Submarine Warfare
B2B	Business to Business
BCA	Business Case Analysis
BOR	Board of Representatives
BPA	Blanket Purchase Agreement
BSA	Baseline Systems Assessment
BSC	Balanced Scorecard
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
C&A	Certification and Accreditation
CA	Certification Authority
CAC	Common Access Card
CADM	Core Architecture Data Model
CASE	Computer Aided Software Engineering
CCA	Clinger-Cohen Act of 1996
CD	Compact Disc
CDRL	Contract Data Requirements Lists
CEO	Chief Executive Officer
CHINFO	Chief of Information
CIAO	Critical Infrastructure Assurance Officer
CINPACFLT	Commander in Chief, U.S. Pacific Fleet
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPIS	Critical Infrastructure Protection Integration Staff
CIPP	Critical Infrastructure Protection Plan

CKO	Chief Knowledge Officer
CLIN	Contract Line Item Number
CMC	Commandant of the Marine Corps
CNA	Center for Naval Analysis
CNET	Chief of Naval Education and Training
CNL	Consortium of Naval Libraries
CNO	Chief of Naval Operations
CoI	Community of Interest
CONSSATL	Council of Scientific, Special, and Technical Librarians
CONUS	Continental United States
COOP	Continuity of Operations
CoP	Community of Practice
COTF	Commander, Operational Test & Evaluation Force
COTS	Commercial Off-the-Shelf
CPAM	CNO's Program Analysis Memorandum
CPG	Career Path Guide
CPP	Career Progression Plan
CPT	Career Planning Tool
CT	Computerized Tomography
CT	Connecting Technology
CTE	Compliance Test and Evaluation
CTF	Commander Task Force
CVBG	Carrier Battlegroup
DAB	Defense Acquisition Board
DARPA	Defense Advanced Research Projects Agency
DASN(C41/EW/ SPACE)	Deputy Assistant Secretary of the Navy (Command, Control, Communications, Computers, Intelligence, Electronic Warfare, and Space)
DCIO	Deputy Chief Information Officer
DEERS	Defense Eligibility Enrollment Reporting System
DENCAS	Dental Common Access System
DEPSECDEF	Deputy Secretary of Defense
DI	Defense Infrastructures
DIAD	DON Integrated Architecture Database
DiD	Defense in Depth
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DL	Distributed Learning
DMI	Data Management & Interoperability
DMIR	Data Management & Interoperability Repository
DMS	Defense Messaging System
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DoD IG	DoD Inspector General's Office

DON	Department of the Navy
DON CIO	Department of the Navy Chief Information Officer
DONPIC	Department of Navy Program Information Center
DPG	Defense Planning Guidance
DPSB	DON Program Strategy Board
DRPM	Direct Reporting Program Manager
DTIC	Defense Technical Information Center
E3	Electromagnetic Environmental Effects
EA	Enterprise Architecture
EAG	Enterprise Action Group
EAMIT	Enterprise Architecture Manager of Information Technology
eBusiness	Electronic Business
ECA	External Certification Authority
ECM/ECCM	Electronic Countermeasures/Electronic Counter-Countermeasures
EDI	Electronic Data Interchange
EDS	Electronic Data Systems
eGov	Electronic Government
EIP	Enterprise Information Portal
EIT	Electronic and Information Technology
EKMT	Enterprise Knowledge Management Taxonomy
EMI	Electromagnetic Interference
EPIC	Electronic Privacy Information Center
ERM	Electronic Records Management
ERMA	Electronic Records Management Application
ERMS	Electronic Records Management System
ERP	Enterprise Resource Planning
ESG	Executive Steering Group
EW	Electronic Warfare
ExecBd	Executive Board
FAIR Act	Federal Activities Inventory Reform Act of 1998
FAQ	Frequently Asked Questions
FAR	Federal Acquisition Regulation
FARA	Federal Acquisition Reform Act
FDMs	Functional Data Manager
FIPS	Federal Information Processing Standards
FIRMR	Federal Information Resources Management Regulation
FMB	Office of Budget and Fiscal Management
FOC	Full Operational Capabilities
GAO	General Accounting Office
GIG	Global Information Grid
GISRA	Government Information Security Reform Act
GNIE	Global Networked Information Enterprise
GPRA	Government Performance and Results Act
GPRS	General Packet Radio Service
GPS	Global Positioning System

GSA	General Services Administration
GSM	General Services for Mobile
HR	Human Resources
I&W	Indications & Warnings
IA	Information Assurance
IAVA	Information Assurance Vulnerability Assessment
IBM	International Business Machines
IC CIO	Chief Information Officer, Intelligence Community
IDS	Intrusion Detection System
IEC	Information Executive Committee
IECA	Interim External Certification Authority
IER	Information Exchange Requirement
IG	Inspector General
IKM	Institute for Knowledge Management
IL	Information Literacy
ILC	Information Leadership Council
ILS	Integrated Library System
IM	Information Management
IM/IT	Information Management and Information Technology
IMSP	Information Management Strategic Plan
INE	In-line Network Encryptors
IO	Information Operations
IOC	Initial Operational Capability
IP	Internet Protocol
IPT	Integrated Product or Process Team
IR3B	Integrated Resources & Requirements Review Board
IRAC	Interdepartment Radio Advisory Committee
IRM	Information Resources Management
ISF	Information Strike Force
ISO	International Organization for Standardization
IT	Information Technology
IT-21	Information Technology for the 21 st Century
ITDB	Information Technology Database
ITIA	Information Technology Infrastructure Architecture
ITMRA	Information Technology Management Reform Act
ITP	Interoperability Test Plan
ITSG	Information Technology Standards Guidance
IWAR	Integrated Warfare Architecture
JITC	Joint Interoperability Test Command
JPO-STC	Joint Program Office for Special Technology Countermeasures
JROC	Joint Requirements Operational Capabilities
JSC	Joint Spectrum Center
JTA	Joint Technical Architecture
KCO	Knowledge Centric Organization
KEG	Knowledge Exchange Gateway
KID	Knowledge, Information, and Data

KM	Knowledge Management
KMAT	Knowledge Management Assessment Tool
KMI	Key Management Infrastructure
LAN	Local Area Network
LCD	Liquid Crystal Display
LOCC	Library of Congress Classification
MAIS	Major Automated Information System
MC	Marine Corps
MCTF-CND	Marine Corps Task Force for Computer Network Defense
MCTN	Marine Corps Tactical Network
MDA	Milestone Decision Authority
MDAPs	Major Defense Acquisition Programs
METOC	Meteorology and Oceanography
MRI	Medical Resonance Imaging
MSC	Commander, Military Sealift Command
NAF	Naval Air Facility
NAICS	North American Industrial Classification System
NAPA	National Academy of Public Administration
NARA	National Archives and Records Administration
NAS	Naval Air Station
NAS	Naval Audit Service
NAVAIR	Naval Air Systems Command
NAVSEA	Naval Sea Systems Command
NAVSUP	Naval Supply Systems Command
NCC	Navy Communications Center
NCIS	Naval Criminal Investigative Service
NCTF-CND	Navy Component Task Force for Computer Network Defense
NFS	Network File System
NIST	National Institute of Standards and Technology
NMCI	Navy Marine Corps Intranet
NOC	Network Operations Center
NSS	National Security Systems
NSTISSC	National Security Telecommunications and Information Systems Security Committee
OASN (FM&C)	Office of the Assistant Secretary of the Navy (Financial Management and Comptroller)
OGC	Office of General Counsel
OMB	Office of Management and Budget
ONR	Office of Naval Research
OPA	Office of Program Appraisal
OPLAN	Operation Plan
OPM	Office of Personnel Management
OPNAV	Office of the Chief of Naval Operations
OSD	Office of Secretary of Defense
OT&E	Operational Test & Evaluation

OUSN (ASP/I)	Assistant for Special Programs and Intelligence, Office of the Under Secretary of the Navy
P&R	Programs and Resources
PA	Privacy Act of 1974
PACFLT	Pacific Fleet
PDA	Personal Digital Assistant
PDD	Presidential Decision Directive
PDR	Post-Deployment Review
PEO	Program Executive Officer
PEO(IT)	Program Executive Officer for Information Technology
PIA	Privacy Impact Assessment
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PM	Program Manager/Program Management
POM	Program Objective Memorandum
PPBS	Planning, Programming and Budgeting System
PRA	Paperwork Reduction Act
RAPIDS	Real-Time Automated Personnel Identification System
R&D	Research and Development
RASP	Remote Access Security Program
RF	Radio Frequency
RMA	Records Management Application
RTC	Recruit Training Command
SAM	Software Asset Management
SATCOM	Satellite Communications
SBU	Sensitive But Unclassified
SCO	Smart Card Office
SECNAV	Secretary of the Navy
SLA	Service Level Agreement
SME	Subject Matter Expert
SPAWAR	Space and Naval Warfare Systems Command
SSIC	Standard Subject Identification Code
SSL	Secure Sockets Layer
STRDTE	Science & Technology, Research & Development, Test & Evaluation
SYSCOM	Systems Command
T&E	Test and Evaluation
TCO	Total Cost of Ownership
TCP/IP	Transmission Control Protocol/Internet Protocol
TES	Technology Enablement Strategies
TFWeb	Task Force Web
TOC	Total Ownership Cost
TREC	Text Retrieval Conference
UAV	Unmanned Aerial Vehicle
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics

USD(C)	Under Secretary of Defense (Comptroller)
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USMC I&L	Deputy Chief of Staff for Installations & Logistics
USMC I	Deputy Chief of Staff for Intelligence
USMC P&R	Deputy Chief of Staff for Programs & Resources
USMC PP&O	Deputy Chief of Staff for Plans Policies & Operations
VCNO	Vice Chief of Naval Operations
VO	Verifying Official
WAN	Wide Area Network
WRC	World Radio Conference
XML	Extensible Markup Language
Y2K	Year 2000

Glossary

A

Action Learning

A process in which participants plan an action, carry it out, reflect upon it, and share that reflection in a group session as they plan to carry out the action again and improve it.

Agents (Agent Technology)

Software program that transparently executes procedures to support gathering, delivering, categorizing, profiling important, or notifying the knowledge seeker about the existence of or changes in an area of interest.

Architecture Framework, DoD

An architecture framework provides a consistent means of documenting the enterprise information technology architecture. The framework specifies graphical and textual formats for capturing information flow, data formats, systems connectivity, and technical standards. Within the Department of Defense, the DoD Architecture Framework specifies the products needed to support three separate, but interrelated views of the architecture: (1) Operational: a description of the tasks and activities, operational nodes, and information exchange requirements between nodes. The Operational view is technology-independent. (2) Systems: a graphical and textual description of systems and interconnections used to satisfy the operational needs described in the Operational view. (3) Technical: the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements.

Asset

Any Military/private/commercial resource, relationship, instrument, installation, supply or system that in some combination is used in a Military operational or support role. Can be CONUS or OCONUS (SECNAVINST 3501.1, CIP).

B

Balanced Scorecard

An approach to gauging the performance of an organization, project, or system that takes into account measures from five perspectives: Stakeholders, Customers, Internal Business Processes, Financial, and Learning and Growth.

Benchmarking

The process whereby one action, product, or service becomes the reference point from which similar actions, products, or services are measured.

Best Practices

Practices that are considered to be superior in approach and results. This information can take the form of processes, studies, surveys, benchmarking, and research. They represent subject matter experts' (SME) experiences, research, and industry knowledge. Best Practices often apply to many different environments and organizations.

Biometric

Automated method of authenticating or verifying an individual based upon a physical or behavioral characteristic.

Bot

A program used on the Internet that performs a repetitive function such as posting a message to multiple newsgroups or searching for information or news. The term is used for all variety of macros and intelligent agents that are Internet or Web related.

Browser

Short for Web browser, a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Another name for a client program that allows users to access documents on the World Wide Web. Browsers can be both text-based and graphic.

Business-to-Business (B2B)

This term is often used to describe Web sites that sell services to other businesses. Thus, businesses are serving other businesses as opposed to consumers.

C

Capital Planning

A process for the effective selection, management, and evaluation of IT investments. (The DON IM/IT Capital Planning Guide is a tool developed by the DON CIO, that outlines the DON's capital planning policies and procedures, and provides a model to assist managers and decision-makers with the capital planning process).

Certificate, Digital

An electronic credential used to identify individuals when doing business or other transactions electronically. It is issued by a certification authority (CA). It contains an individual's name, public key, a serial number, expiration dates, and additional data.

Chief Knowledge Officer (CKO)

Manages the knowledge sharing process at the command level; leads efforts to move the organization to knowledge centrality; requires a dedication to knowledge management principles, the ability to discuss the benefits of knowledge sharing and the vision to ensure that KM initiatives are adopted by the organization; ensures that the best, relevant information for the area of practice is accessible to all personnel and implements the knowledge sharing strategy in alignment with command guidelines; champions cross-organizational communities of practice, and organizational learning; establishes incentive programs for

knowledge sharing and re-use; fosters cultural change; defines roles, skill-set, and opportunities for knowledge workers; and facilitates training and education of knowledge workers.

Clumping

Organizing information and data around decision points to promote efficient and effective decision-making. Clumping is driven by decision-making. When you need to make decisions at the top level, you dig out, down, and around to find the authoritative data fields you need from disparate locations, then you link directly to those fields for continuous real-time feed to support your emerging decision-making requirements.

Clustering

Process of categorization by similarities when you bring data and information together that are similar or related, i.e. first and second cousin organization. Clustering supports ease of locating specific data and can lead to innovation and insights.

Collaboration

Involves two or more people working together in real-time, or in a “store-and-forward” mode. Applications will enable a group of people to collaborate in real-time over the network using shared screens, shared whiteboards, and video conferencing. Collaboration can range from two people reviewing a slide set online to a conference of doctors at different locations sharing patient files and discussing treatment options.

Common Access Card (CAC)

A smart card used as the Department of Defense (DoD) standard identification card. It is replacing existing Military and Civilian personnel identification cards, and will be used as the DoD’s authentication token. The new CAC combines multiple technologies on a single plastic card, including: a microcomputer based on an embedded integrated circuit computer chip; a magnetic strip; a barcode; and a photograph. The CAC will be the principle card used to enable physical access to buildings and controlled spaces, and will be used to enable information technology systems and applications that access the Department’s computer networks. The new CAC will be issued to active duty and selected Reserve personnel, DoD Civilian employees, and eligible DoD contractor personnel.

Community of Interest

Groups or individuals with a common interest. This interest does not necessarily relate to their day-to-day work or current tasking. Communities of interest may share ideas and communicate or collaborate.

Communities of Practice

A group of individuals who share a common working practice over a period of time, though not a part of a formally constituted work team. Communities of practice generally cut across traditional organizational boundaries and enable individuals to acquire new knowledge at a faster rate.

Competency Management

The ability to use knowledge management to consistently facilitate the formation of new ideas, products, and services that support the core competency of the organization.

Concept of Operations

A document detailing the method, act, process, or effect of using an information system or performing a function.

Concept-Based Search

A form of content-based indexing, search, and retrieval in which the search engine possesses a level of intelligence regarding semantics and lexicons. In such a system, internalization and externalization can be achieved at a conceptual level, providing results far beyond that of world-based queries.

Context Sensitivity

The ability of a knowledge management system to provide information and connections by taking into consideration the contextual nature of a user's request based on history, associations, and subject matter experience.

Continuous Learning

Continuous Learning infers to continuous cognitive or behavioral activity between an individual and their environment. In teams and organizations, continuous learning is a collective process dependent upon relationships and interactions among individuals.

Contribution Process

The act of capturing, codifying, and submitting content to the knowledge repository through four important roles: knowledge administrator, subject matter expert (SME), knowledge contributor, and knowledge champion.

Cookie

Small piece of information (token) sent by a Web server and stored on a user's system (hard drive) so it can later be read back from that system. Cookies can help Web sites maintain user-specific information and preferences to enhance the users' Web-surfing experience. However, when implemented and used inappropriately by Web sites, cookies can pose a threat to user privacy. Users can tailor their browser to refuse cookies, although that may affect use of some Web sites.

There are two kinds of cookies:

a. Session Cookie—Temporary cookies that are used to maintain context or “state” between otherwise stateless Web transactions (e.g., to maintain a “shopping basket” of goods selected during a single logical session at a site) and that must be deleted at the end of the web session in which they are created.

b. Persistent Cookies—Remain over time and can be used for a variety of purposes, including to track a user's access over time and across Web sites, or to establish user preferences.

Core Competency

The overriding long-term value source of an organization. Core competency differs from product and market competency in that an organization's core competency outlives (by a significant margin) product life cycles and market swings.

Corporate Capital

Includes intellectual property, both formal and informal (i.e. patents, ideas), corporate functional and organizational processes. It also includes all the data and information captured in corporate databases and all that we can visibly get our hands around and all that has been made explicit. The challenge for an organization is to fully leverage this capital through sharing, collaborating, innovating, and learning. Corporate capital is one of the components of intellectual capital, along with human capital and social capital.

Critical Assets (see also Asset)

An asset identified as performing an essential service, function or use to the US Military whose disruption or loss would render DoD Critical Assets ineffective or otherwise seriously disrupt DoD operations (SECNAVINST 3501.1, CIP).

Critical Infrastructures

Those physical and cyber-based systems needed to operate the economy and government. These systems include: telecommunications, energy, banking and finance, transportation, water systems, and emergency services—both government and private.

Cryptographic Hardware Token

A device (smart card, USB plug, PCMCIA card, module/PC board, etc.) which implements approved security functions which may include cryptographic algorithms and key generation.

D

Data

(1) A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. (2) Data are distinct pieces of information, usually formatted in a special way. All software is divided into two general categories: data and programs. Programs are collections of instructions for manipulating data.

Data Mining

A hot buzzword for a class of database applications that look for hidden patterns in a group of data. For example, data mining software can help retail companies find customers with common interests. The term is commonly misused to describe software that presents data in new ways. True data mining software doesn't just change the presentation, but actually discovers previously unknown relationships among the data.

Data Warehouse

A collection of data designed to support management decision-making. Data warehouses contain a wide variety of data that present a coherent picture of business conditions at a single point in time. Development of a data warehouse includes development of systems to extract data from operating systems plus installation of a warehouse database system that provides managers flexible access to the data. The term data warehousing generally refers to combining many different databases across an entire Enterprise.

Decision Grounding

The process of verifying or vericating decisions.

Decision Support Systems

Information databases or other software that is accessible to employees and designed to assist them in making quick decisions. The primary objectives of decision support systems are to give employees the tools to make informed decisions, and to prevent delays previously caused by routing questions up a defined organizational hierarchy.

Defense in Depth

The Military strategy to employ several simultaneous layers of defense so that an attacker must successfully compromise each and every layer in order to compromise the system being protected.

Defense Technical Information Center (DTIC)

DTIC is the central Department of Defense facility for providing access to and facilitating the exchange of scientific and technical information produced at taxpayer expense. DTIC databases contain citations to, or full text of, a vast quantity of documents, some of them security classified. US Government organizations and their contractors are eligible to register for DTIC's products and services. Many of the unclassified documents in DTIC's collections are available to the general public through the National Technical Information Service (NTIS). DTIC has created and hosts over 80 Internet Web sites for various organizations.

Digital Divide

Refers to the gap that exists between those who can afford technology and those who cannot.

Discernment and Discretion

In the capital information age, the act of selecting, valuing and laying aside information; i.e., the ability to identify and choose what is of value, and the equally difficult ability to toss aside what is not of value.

Discussion Database

A running log of remarks and opinions about a subject. Users post their comments and the computer maintains them in order of originating message and replies to that message.

Distance Learning

See Distributed Learning

Distributed Learning

Structured learning that takes place without requiring the physical presence of an instructor. Distributed learning is synchronous and/or asynchronous learning mediated with technology and may use one or more of the following media: audio/videotapes, CDs, audio/video-teletraining, correspondence courses, interactive television, and video conferencing. Often referred to as "eLearning."

Document Management

Document management is a term used to refer to the storage, retrieval, tracking, and administration of documents within an organization. Its primary origin was the use of manual file cabinets to store paper-based documents in alphabetized categories based on the document's contents. Since the widespread use of computer technologies, document management now also applies to electronic documents and paper-based documents that have been converted to electronic form. These electronic documents exist in a variety of formats to include word-processing files, spreadsheets, graphics, video, audio, bit-mapped images, and compound documents incorporating multiple formats. Now, instead of manual file cabinets, document management software is required to provide users with services to access electronic documents.

Dot Com

Refers to companies that were formed to offer services or products on the Web. Literally refers to the period (dot) followed by the abbreviation of the commercial domain (.com) at the end of a Web address.

E

eBusiness (eB, Electronic Business)

The interchange and processing of information via electronic techniques for accomplishing transactions based upon the application of commercial standards and practices. Further, an integral part of implementing eB is the application of business process improvement or reengineering to streamline business processes prior to the incorporation of technologies facilitating the electronic exchange of business information.

eCommerce

The buying and selling of goods and services on the Internet, especially the World Wide Web. Often this term and the term, eBusiness are used interchangeably. In practice, eCommerce is usually restricted to the process of buying, selling, and paying; eBusiness refers to the digitalization of a vast area of business processes. For on line retail selling, the term eTailing is sometimes used.

eGovernment

The access to and interchange of government information via the Internet and electronic media. In the DON specifically related to the combination of knowledge management and eBusiness, enabled government...government of the people, by the people and for the people in a virtual world, a collaborative government where technology meets human creativity, and where government manages and shares its vast stores of knowledge with, and for the benefit of, the citizens.

eLearning

See Distributed Learning

eMarketplace

A Web site that enables buyers from many suppliers by combining state-of-the-art technology, industry best practices, and best price products and services to provide “point and click” comparison shopping. eMarketplaces provide decision support tools that enable a buyer to make the most informed decision and support various procurement methods such as reverse auction technology.

EDI (Electronic Data Interchange)

The computer-to-computer exchange of business data in a standardized format between entities.

EIP (Enterprise Information Portal)

An Internet gateway that provides proprietary, Enterprise-wide information to company employees, as well as access to selected public Web sites and vertical-market Web sites (e.g., suppliers, vendors). EIP includes a search engine for internal documents, as well as the ability to customize the portal page for different user groups and individuals. It is the internal equivalent of the general-purpose portal on the Web.

Electromagnetic Spectrum

The entire range of light radiation, from gamma rays to radio waves. The ability of Naval forces to support diverse operations and crises is largely dependent on their ability to communicate using the electromagnetic spectrum.

Enterprise

Literally, it refers to the entire organization. In DON that is the Fleet and the infrastructure, including all Military and Civilian personnel. In the computer industry, the term is often used to describe any large organization that utilizes computers. An intranet is a good example of an enterprise computing system.

Enterprise Architecture

Documentation of current and desired relationships between business process/warfighting activities and the supporting information technology.

Enterprise Knowledge

Enterprise knowledge covers all intellectual capital the Enterprise has (both implicit and explicit), and includes three essential components: human capital, social capital and corporate capital. See definitions of these three components.

Enterprise Licensing

A method of purchasing commercial software that leverages the vast buying power of the DoD. Enterprise licensing consolidates software requirements across the DoD or DON and negotiates enterprise software agreements (ESA) with software vendors, thereby realizing significant total cost of ownership (TCO) savings in software acquisition and maintenance.

Enterprise Portal

A gateway for single point access to all DON information management systems as well as connectivity to other government and commercial Web sites.

Expert System

A computer system designed based on rules (e.g., “if-then” statements) to emulate a human expert to help knowledge workers solve problems. A typical expert system has three main parts: a knowledge base (which contains rules), an inference engine (which interprets the situation against the rules), and a human interface.

Explicit Knowledge

Formal, systematic knowledge that is easily identified, in times such as policy, operation, and procedure manuals, without vagueness or ambiguity.

External Scanning

Using intelligent agent software or individuals to continuously survey available information sources to retrieve information that has been deemed important.

Extranet

A private wide area network (WAN) running on public protocols. The goal of most extranets is to foster collaboration and information sharing between two or more organizations. Extranets make it possible for organizations to invite selected guests to have access to their internal data through a Web browser rather than proprietary software tools. Selected guests might include customers, corporate colleagues working around the globe, or other organizations.

F

Federal CIO Council

The principal interagency forum to improve agency practices for the management of information technology.

Federal Knowledge Management Working Group

Self-managed cross organizational Federal working group sponsored by the Federal CIO Council that facilitates the sharing of knowledge and expertise across government.

Filtering

The process of taking contributions/content from the divergent part of the knowledge base system and moving it to the convergent part of the system, providing the most relevant knowledge for that subject domain.

FirstGov Portal

Government Web page that serves as a point of entry for World Wide Web users.

Flow

See Knowledge Flow

Full Dimensional Protection

The ability of the joint force to protect its personnel and other assets required to decisively execute assigned tasks.

G

General Packet Radio Service (GPRS)

A standard for wireless communications which runs at speeds up to 150 kilobits per second, compared with current GSM (Global System for Mobile Communications) systems' 9.6 kilobits. GPRS, which supports a wide range of bandwidths, is an efficient use of limited bandwidth and is particularly suited for sending and receiving small bursts of data, such as e-mail and Web browsing, as well as large volumes of data.

Global Information Grid

The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

H

Home Page

The first page on a Web site that acts as the starting point for navigation.

Human Capital

The ability of individuals to apply solutions to customers' needs through attributes, competencies, and mindsets. All the expertise, experience, capability, capacity, creativity, adaptability, etc., possessed by the individuals in an organization.

Hyperlink

An electronic path that connects two places in a network, often represented as buttons or pointers on the World Wide Web.

Hypertext

A type of text that allows embedded "links" to other documents. Clicking on or selecting a hypertext link displays another document or section of a document. Most World Wide Web documents contain hypertext. Also, a set of interactive files in which the individual works link one file to the next.

HTML

The document format used on the World Wide Web. Web pages are built with HTML tags, or codes, embedded in the text. HTML defines the page layout, fonts and graphic elements as well as the hypertext links to other documents on the Web. Each link contains the URL, or address, of a Web page residing on the same server or any server worldwide, hence "World Wide" Web. HTML is not a programming language like Java or JavaScript (if this, do that); rather it could be considered a "presentation language." HTML is derived from SGML, the standard generalized markup language, which is widely used to publish documents. HTML is an SGML document with a fixed set of tags that, although change with each new revision, are not flexible.

I

Information

(1) Facts, data, or instructions in any medium or form. (2) The meaning that a human assigns to data by means of the known conventions used in their representation (Joint Pub 1-02). (3) Data that has been arranged in meaningful patterns; synthesized data.

Information Assurance

Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Literacy

Information age skills that enable individuals to recognize when information is and is not needed and how to locate, evaluate, integrate, use, and effectively communicate needed information.

Information Operations

Those actions taken to affect an adversary's information and information systems while defending one's own information and information systems.

Information Superiority

The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information System

The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Information Technology (IT)

Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term "equipment" in this definition means equipment used by a Component directly, or used by a contractor under a contract with the Component, which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. The term "IT" includes National Security System (40 U.S.C. 1401 and reference (a), Sec 5002).

Intangible or Intellectual Assets

Anything of value without physical dimensions that is embedded in people (employees, customers, and suppliers) or derived from processes, systems, and culture associated with an organization.

Integrative Competencies

A set of fundamental skills and abilities that enhance working and living in a virtual world. These competencies have a multiplier effect through their capacity to enrich an individual's cognitive abilities and enable connectivity and integration of other competencies, leading to improved understanding, performance, and decisions.

Intellectual Capital

The value created by the use of the human intellect. It represents the intangible assets of an organization and includes human capital, social capital, and corporate capital. Intellectual capital is the essence of knowledge management (KM) at the Department of the Navy.

Intermediation

The process of linking disparate knowledge providers with people in need of the knowledge, both inside and outside the organization. People who are involved in this process are called knowledge intermediaries or knowledge brokers in the knowledge marketplace. Intermediaries play roles similar to a stock broker in the stock market. Intermediaries help people assess knowledge, and maintain the relevancy of the knowledge base.

Internalization

The process of embodying explicit knowledge into tacit knowledge; closely related to "learn by doing."

Internet

A worldwide system of computer networks in which users at any one computer can get information from any other computer. Today it is a public, cooperative, and self-sustaining facility accessible to hundreds of millions of people worldwide.

The loosely connected worldwide collection of computer systems that uses a common set of communications standards to send and receive electronic information.

Internet Protocol (IP)

The numeric address that is translated into a domain name by the Domain Name System (DNS).

Interoperability

The ability of two or more hardware devices or two or more software routines to work together. For example, routers and switches in a network require interoperability. The term is more often used with hardware than with software.

Intranet

A computer network designed to meet the internal needs of a single organization or company that is based on Internet technology (TCP/IP). Not necessarily open to the external Internet and almost certainly not accessible from the outside, an intranet enables organizations to make internal resources available using familiar Internet clients, such as web browsers, newsreaders, and e-mail.

ISO Standard

International agreement or standard set by the International Organization for Standardization (ISO), a worldwide federation of national standards bodies. ISO standards

facilitate the international exchange of goods and services, and develop cooperation in intellectual, scientific, technological and economic activity.

IT-21 (Information Technology for the 21st Century)

Department of the Navy's afloat information technology capability.

K

Knowledge

The potential and actual ability of a human to take action.

Knowledge Assets

Intangible assets that consist of the thought or logic behind the product.

Knowledge Audit

A process to determine how information is collected, stored, and reported, and how the reports are used. A knowledge audit looks at what information is available and what is used.

Knowledge Base

Stored information and expertise of individuals within the organization that can be accessed by users.

Knowledge-Centric Organization

A knowledge-centric organization (KCO) is one that organizes virtually around its critical knowledge needs and then builds useful and relevant information to fill those needs. This virtual organization is an overlay to the existing organizational structure; personnel integrate knowledge sharing into their everyday lives. By providing access to the breadth of organizational knowledge, people have the ability to quickly and accurately draw upon critical lessons learned to make work time more efficient. The bottom line is the knowledge workers will be up and running faster and more effectively than ever before.

Knowledge Champion

The person responsible for the overall knowledge management effort. This person has the authority to enforce rules related to knowledge management and is in a position of leadership within the organization.

Knowledge Ecology

An interdisciplinary field of management theory and practice, focused on the relational and social/behavioral aspects of knowledge creation and utilization. Its primary study and domain of action are the design and support of self-organizing knowledge ecosystems, providing the infrastructure in which information, ideas, and inspiration can travel freely to cross-fertilize and feed on each other.

Knowledge Economy

A recently coined term that refers to the stage of economic evolution in which knowledge, rather than land, labor, and capital, is the key factor of production. This major change has

significant implications for the strategy, operations, and organizational structure of a business enterprise. The knowledge economy was preceded by the industrial age, which was preceded by the agricultural age.

Knowledge Fair

A fair held to create awareness of knowledge management and facilitate knowledge sharing. Considered an event-driven knowledge intermediation.

Knowledge Flow

Knowledge moving networks of systems and people, shared through teams, communities, and events. This flow is facilitated through knowledge repositories and portals, enabling knowledge-centricity. An illustrative representation is information flowing in and out of a process, capturing the owners and recipients of the information.

Knowledge Inventory

The systemic identification of an organization's knowledge. Since such knowledge is often intact, the inventory may often be "pointers to people" rather than knowledge itself.

Knowledge Management

The process for optimizing the effective application of intellectual capital (human capital, social capital, and organizational capital) to achieve organizational objectives. This process ensures the decision-maker has the ability to use the best information available when and where it is needed.

Knowledge Management System

A type of system that facilitates communications and knowledge-sharing within an organization. The system can acquire, store, and deliver knowledge and experience to knowledge workers.

Knowledge Mapping

The visual display of captured information and relationships that enable the communication and learning of knowledge by observers with differing backgrounds at multiple levels of detail. The individual items of intellectual capital included in such a map can be text, stories, graphics, models, or numbers. Maps can also serve as links to more detailed knowledge sources as well as pointers to implicit knowledge such as experts.

Knowledge Market

An online gathering place where owners of intellectual property can barter, sell, and otherwise exchange their intellectual property for value. Such markets may be undifferentiated (e.g., knowledge bazaars), organized through knowledge brokers, or modulated.

Knowledge Object

A complete, discrete package of information/content that has stand-alone meaning. Examples include: (1) a spreadsheet that is programmed to perform complex financing calculations, and (2) a casual loop diagram that describes a complex industrial process. Knowledge objects enable the user to be more productive and illustrate the thinking of their author.

Knowledge Strategy

A discussion/description of: (1) how knowledge will contribute to a company's competitive advantage, (2) important knowledge categories that need to be created and shared, and (3) a plan for acquiring and using knowledge that addresses people, process, and technological issues.

Knowledge Superiority

Shared understanding which allows us to deter, shape or dominate an adversary. It provides a decisive edge in warfighting, greatly enhances our business processes, and vastly improves the individual productivity of our people. Knowledge superiority is achieved through a holistic, synergistic, robust and adaptive system of people, information and equipment.

Knowledge Systems

Knowledge systems embody within them general forms of reasoning and rules (i.e., case-based and rule-based reasoning), which then permit the system to analyze a new situation or process, finding similarities to existing case or relevance to existing rules.

Knowledge Worker

A worker whose job depends on the processing and use of information in a continuously changing work environment. The responsibility to make recommendations and provide value-added solutions is what differentiates a knowledge worker from a service worker.

L

Learning

An enduring change in behavior or in the capacity to behave in a given fashion, which results from practice or other forms of experience. Learning in organizations means the continuous testing of experience and the transformation of that experience into knowledge—accessible to the whole organization and relevant to its core purpose.

Learning History

Retrospective documents, usually based on a series of interviews and told in the participants' own words using quotes from the interview process. Designed to pass along information as a means of surfacing issues and dynamics within groups.

Learning Organizations

An organization that is committed to continuous learning. This applies to both individuals in their personal development and at the organizational level. The DON Continuous Learning Guidance was issued on July 11, 2000 by a DON CIO memorandum.

Legacy System

A system or application in which an organization has already invested considerable time and money. Typically, legacy systems are database management systems (DBMSs) running on mainframes or minicomputers. An important feature of new software products is the ability to work with existing legacy systems or at least be able to import data from them. These systems may be candidates for phase-out, upgrade, or replacement.

M

Major Acquisition Information System (MAIS)

An AIS acquisition program that is: (1) designated by Assistant Secretary of Defense (C3I) as a MAIS, or (2) estimated to require program costs in any single year in excess of 30 million in fiscal year (FY) 1996 constant dollars, total program costs in excess of 120 million in FY 1996 constant dollars, or total life cycle costs in excess of 360 million in FY 1996 constant dollars. MAISs do not include highly sensitive classified programs (as determined by the Secretary of Defense).

Mentoring

Training programs or apprenticeship relationships, where new recruits are assigned to a more experienced employee to help them adapt to the new business environment. Mentoring and coaching relationships can help maintain the balance of knowledge transfer modes within an organization, such that learning is not solely expected to happen through explicit training courses, manuals, etc.

Meta-Data

Information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings.

Meta Tag

An HTML tag that identifies the content of a Web page. Using <meta name=" " content=" "> format, meta tags contain such items as a general description of the page, keywords for search engines, and copyright information.

N

National Security Systems (NSS)

Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of Military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is subject to subsection; or is critical to the direct fulfillment of Military or intelligence missions.

Navy Marine Corps Intranet (NMCI)

A performance-based, Enterprise-wide services contract that incorporates future strategic computing and communications capability and is managed much the same as any other "utility," like water, telephone, gas, and electricity, paying for the service as it is delivered.

O

Ontology

The conceptual framework that people are really trying to express in a classification scheme. The ontology is translated into a hierarchy of descriptive categories that form the taxonomic schema used to control the classification process.

Open Standards

Standards used in open systems that call for sufficient interfaces, services, and supporting formats to enable properly engineered components to be utilized across a wide range of systems with minimal changes, to interoperate with other components on local and remote systems, and to interact with users in a style that facilitates portability.

P

Performance Measurement

The standards used to measure success in achieving an objective. Performance measures describe the precise measurement that will generate a quantitative (or qualitative) indicator that explicitly or implicitly indicates progress towards achieving the objective.

Personal Digital Assistant (PDA)

A handheld computer that serves as an organizer for personal information. It generally includes at least a name and address database, to-do list and note taker. PDAs are pen based and use a stylus to tap selections on menus and to enter printed characters. The unit may also include a small on-screen keyboard which is tapped with the pen. Data is synchronized between the PDA and desktop computer via cable or wireless transmission. A PDA is like a palmtop computer except that the PDA typically uses a pen whereas the palmtop uses a small keyboard. Apple's MessagePad, more commonly known as the "Newton," was the first to popularize the concept.

Privacy Impact Assessment (PIA)

An assessment methodology used to evaluate and ensure adequate privacy practices of an organization. The process is designed to guide owners and developers of information systems in assessing privacy throughout the life cycle of the system. The process consists of privacy training, gathering specific data on information systems, identifying and resolving the privacy risks, and approval by a designated privacy representative.

Public Key Infrastructure (PKI)

Framework of laws, policy, procedures, and technologies for the use of digital credentials, which provide confidentiality, integrity, authenticity, and non-repudiation in electronic communications and transactions. PKI is the service that validates, issues, and revokes digital credentials for objects.

Q–R

Reach-Back Capability

The ability of deployed forces in a forward deployed or remote site to effectively and expeditiously access timely information from the home base or other information repository that is required for or aids in the execution of their mission.

Records Management

The planning, controlling, directing, organizing, training, promoting and other managerial activities involved with respect to records creation, records maintenance and use and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

Reverse Auction

“Downward-price” auctions in which suppliers continue to lower their prices until the auction closes. Buyers watch as competitors lower price in real time. The first Internet reverse auction in the Federal Government was conducted by the DON.

Risk Management

Process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected.

S

Section 508, Rehabilitation Act

The Accessibility Standards, Section 508, Rehabilitation Act Amendments of 1998. Section 508 requires that Federal agencies must ensure comparable accessibility to persons with disabilities whenever that agency uses electronic or information technology, unless such access would impose an undue burden.

Smart Card

A credit card-size device, normally for use by personnel, that contains one or more integrated circuits and may also employ one or more of the following technologies: magnetic strip; bar codes, linear or two-dimensional; non-contact and radio frequency transmitters; biometric information; encryption and authentication; and photo identification.

Smart Card Senior Coordinating Group (SCSCG)

A governing body established by the DoD to develop and implement department-wide interoperability standards for use of smart card technology and a plan to exploit smart card technology as a means for enhancing readiness and improving business processes. This group reports to the DoD CIO.

Social Capital

Includes human and virtual networks, relationships, and interactions across networks built on those relationships. Social capital takes into account all the aspects of language, including context and culture, formal and informal language, and verbal and non-verbal. It includes an element of patterning that deals with timing and sequencing of exchange as well as the density and diversity of the content (i.e., how much, how often, and how intense).

Software Asset Management

A supporting sub-process within IT asset management. It is the cohesive merging of physical, financial and contractual attributes of software to enable the delivery of cost-efficient, timely business solutions. The focus is on managing the software life cycle to reduce costs, reduce liability exposure, improve software license compliance, and better match usage with contract terms. Software asset management complements and extends the IT capital planning process to provide a more effective management structure for enterprise software.

Spectrum Management

The DON's development of technical, business, and operational guidance for proactive spectrum management (see Electromagnetic Spectrum).

Spiral Development Process

A general methodology for developing software that incorporates a cyclic approach into its scheduling and implementation.

Strategic Pause

The three-month pause taken during NMCI implementation by OSD and Congress to assess the effectiveness of the program and determine whether NMCI should proceed to full implementation.

Storytelling

The construction of fictional examples to illustrate a point and effectively transfer knowledge. An organizational story is a detailed narrative of management actions, employee interactions, or other intra-organizational events that are communicated informally within the organization. With the advent of the Internet and intranet, there is a larger opportunity to use stories to bring about change. Electronic media adds moving images and sound as context setters. Hypertext capabilities and collaboration software invite groups, teams, and communities to co-create their stories. When used well storytelling is a powerful transformational tool in organizations, one that all of our managers and leaders across the Department can utilize.

Systems Thinking

An approach for managing complexity by helping decision-makers understand the cause and effect relationships among data, information, and people. It identifies types (or patterns) that occur over and over again in decision-making. Systems Thinking expands individual thinking skills and improve individual decision-making.

T–U

Taxonomy

The classification scheme used to categorize a set of information items. They represent an agreed upon vocabulary of topics arranged around a particular theme.

Trusted Information

Information received or accessed whose source and integrity can be verified through the use of PKI credentials.

V

Verification

To test the reasonableness by consulting a trusted ally; to determine the reasonableness or soundness, validation of information grounded by the implicit.

Virtual Communications

Although virtual is defined as being “unreal,” in the (Information Literacy) ToolKit it refers to communications that take place between one or more individuals across time, place, space and/or distance, using any number of technologies or applications.

W

Work Breakdown Structure

A hierarchical breakdown of processes, activities and tasks for the life cycle of a project.

World Wide Web (WWW)

An Internet facility that links documents locally and remotely. The Web document, or Web page, contains text, graphics, animations, and videos, as well as hypertext links. The links in the page let users jump from page to page (hypertext), whether the pages are stored on the same server or on servers around the world. Web pages are accessed and read via a Web browser, the two most popular being Internet Explorer and Netscape Navigator.

X–Y–Z

XML (Extensible Mark-Up Language)

An open standard for describing data from the World Wide Web. It is used for defining data elements on a Web page and business-to-business documents. It uses a similar tag structure as HTML; however, whereas HTML defines how elements are displayed, XML defines what those elements contain. HTML uses predefined tags, but XML allows tags to be

defined by the developer of the page. Thus, virtually any data items, such as product, sales representative and amount due, can be identified, allowing Web pages to function like database records. By providing a common method for identifying data, XML supports business-to-business transactions and is expected to become the dominant format for electronic data interchange.

Yellow Pages

A listing of individuals, their expertise, and contact information.

Index

- Architecture, 57-63, 90-98, 109, 226, 290
 - DIAD, 94
 - Enterprise, 90-95
 - Infrastructure, 78
 - ITIA, 60, 78-80, 95, 290
 - Policy, 93
- The Art of War*, 191, 286
- Awards, 48-52
- Balanced Scorecard, 124, 265-266, 273, 280, 296
- Capital Planning, 18, 247-262, 264-265, 271, 273-274, 276
 - Evaluation Phase, 249, 258-259, 264, 274
 - Guide, 260
 - Management Phase, 249, 256, 274, 276
 - PPBS, 251-253, 276
 - Selection Phase, 249, 252, 274, 276
- CHIPS Magazine, 54
- CIO, 18, 20-23, 31, 64-66, 68, 71-72
 - Organization, 31
- Clinger-Cohen Act, 17-19, 52, 64-65, 68-69, 86, 240, 250-251, 262, 272
 - CCA Certification, 68
 - CCA Compliance, 68
- Clumping and Clustering, 132, 291-292
- Collaboration, 43, 114, 129, 207, 215, 293, 301, 304-306
 - (See also *Sharing*)
- Common Access Card, 163-170, 225
- Communications and Outreach, 52
- Communities of Practice, 134, 179, 206-208, 304
 - Development Model, 209
 - KM CoP, 134-135, 207-208
- Competencies, 31, 177-178, 181-187, 195, 295, 297
- Congress, 15, 17, 164, 240, 251
- Connectedness of Choices, 26, 58, 287, 292
- Connecting Technology, 47-48
- Consequence Management, 38, 41, 220, 230
- Continuous Learning, 136, 184, 203
 - Guidance, 136, 184, 203
 - (See also Critical Success Factors)
- Critical Infrastructure Protection, 31, 216-217, 228-238, 289-290
 - Activities, 232
 - Council, 231, 233, 235-236
 - Working Group, 230-231, 234-237
- Critical Success Factors
 - Communication and Persuasion, 37, 52, 134, 168, 220
 - Continuous Learning, 37, 54, 136, 146, 184, 191, 203, 207
 - Creativity and Innovation, 36, 47, 81, 124, 126, 167, 238, 269
 - Freedom and Flexibility, 37, 137, 189
 - Hard Work, 38, 76, 80, 168, 218, 270
 - Leadership, 35, 65, 73, 92, 128, 138, 163, 207, 218, 225, 252
 - Managing Change, 35, 47, 123, 131, 169, 220, 264, 283
 - People, 36, 56, 80, 87, 139, 158, 180, 200, 203, 214, 245
 - Quality, 36, 48, 54, 75, 78, 122, 159, 181-182, 186, 194, 196, 238, 244, 260, 261, 264, 273, 276
 - Service, 36, 123, 137, 150, 166, 214
 - Sharing, 37, 47, 54, 126, 129, 135, 186, 194, 196, 205, 206, 208, 260
 - Systems Approach, 36, 73, 78, 130, 154, 181, 189, 219, 224, 263

- Team Approach, 37, 45, 72, 75, 78, 89, 95, 96, 125, 134, 145, 152, 181, 208, 214, 229, 244, 253, 268
- Technology, 36, 66, 98, 124, 138, 148, 167, 183, 212, 225
- Timing, 36, 76, 94, 165
- Critical Thinking, 41, 186, 198
- Culture, 27, 31, 40, 43, 286, 292
- Data Management, 96-98
 - DMIR, 98
 - Policy, 97
- Decision Grounding, 133
- Defense in Depth, 84, 223-225, 242
- Discernment and Discretion, 133
- DoD, 65, 257, 270
 - CIO, 65-66, 68, 71
 - CIO Executive Board, 71
 - Instruction 5000.2, 65, 257
- DON, 231, 285
 - Information Executive Committee, 72
 - Information Leadership Council, 71
 - Posture Statement, 286
 - Vision, 26, 231, 285-287, 298-299
- eBusiness, 49, 118-127, 291, 298
 - Operations Office, 49, 123, 125-126
 - Pilot Program, 126
 - Reverse Auctions, 124
 - Strategic Plan, 122, 125
- Education, 41, 201-205, 244
- eGovernment, 30, 117-120, 303
 - Awards, 48-52, 135
- eLearning, 178, 201-205, 297, 305
 - (See also Learning)
 - Learning in a Virtual World, 186, 204, 297
 - Organizational, 201-205, 297
- Electromagnetic Spectrum, 99-107
- England, Gordon R., Secretary of the Navy, 49
- Enterprise Licensing, 145, 247-248, 267
 - Naval Libraries, 145
- Event Intermediation, 47
- Federal CIO Council, 71
- The Federalist Papers, 70
- The Fifth Discipline, 136, 189, 285
- Forums, 38, 47, 220
 - Expert Forum, 38, 41, 220
 - Industry Forum, 220
- Governance, 70-71
 - DoD CIO Executive Board, 71
 - DON Information Executive Committee, 71, 73-74
 - DON Information Leadership Council, 71-74
 - NMCI Action Group, 72
- Hard Token, 110
- Information Assurance, 84, 216, 222-227, 229, 242-243
- Information Ethics, 198
- Information Literacy, 178, 186, 189, 195-200
- Information Technology
 - (See IT)
- Information Technology for the 21st Century (IT-21), 30, 80, 82, 104, 147
- Infrastructure, 30-31, 57-63, 82, 215, 217, 228-238, 242-243, 288-290, 294
- Innovation, 269, 283-285, 288
 - Life Cycle, 283-284, 288
- Insights, 26, 28, 177, 248, 287, 302
- Integrated Product/Process Teams, 28, 45, 181, 290

-
- DMI, 96, 98
 - IM/IT Workforce, 181
 - ITIA, 95
 - ITSG, 59, 75-77
 - Integrated Vulnerability Assessment, 216, 237-238
 - Integrative Competencies, 178, 186, 189-194
 - Intellectual Capital, 130-131
 - Internet Time, 108-109
 - Interoperability, 64, 78, 85, 303
 - Investment Management, 247, 258, 261-266
 - Investment Evaluation Handbook, 264, 274, 276
 - Investment Portfolio Model, 254
 - Portfolio Management Guide, 261, 263
 - IT, 13, 30-31, 39, 117-119
 - IT Systems, 66, 257
 - MAIS, 257-258
 - Registration, 66
 - Knowing, 191-194, 199, 306-307
 - Definition, 191
 - Knowledge, 30, 40, 128-135, 137-139, 152-162, 286, 288, 290-291, 293, 302-303, 306
 - Life Cycle, 288, 290
 - Knowledge Centric Organization, 134, 139
 - Knowledge Fair, 47-48, 135
 - Knowledge Management, 30, 118-119, 128-140, 147-148, 152-153, 189-190, 276-281, 286-288, 291-294, 298
 - CoP, 134-135, 207-208
 - Definition, 128
 - Framework, 132, 292, 294
 - Implementation, 132, 136
 - Metrics Guide for KM Initiatives, 278, 295
 - Knowledge Superiority, 30-31, 129, 152, 188, 286-287
 - Knowledge Systems, 43, 291, 293
 - Leadership, 53, 92, 218, 286-287, 299
 - (See also Critical Success Factors)
 - Learning, 43, 113, 114-116, 136, 177-178, 189-190, 195-196, 198, 199, 201-205, 292-293, 297, 304-305
 - (See also eLearning)
 - Continuous Learning Guidance, 184, 203, 297
 - Legislation, 15-23, 211-214, 222, 272
 - Clinger-Cohen Act, 17-19, 52, 64-65, 68-69, 86, 240, 250-251, 262, 272
 - Goldwater-Nichols Act, 15
 - Government Information Security Reform Act, 15, 19, 222
 - Government Performance and Results Act of 1993, 272, 277
 - Paperwork Reduction Act, 16, 18-19
 - Section 508, 211-214
 - Section 8102 and 811 of the DoD Appropriations and Authorization Acts, 66, 68
 - Library and Information Services, 141-146, 195
 - Consortium of Naval Libraries, 145, 195
 - Electronic Library, 145
 - Naval Libraries, Technology Impact, 143
 - Limits, 53, 290-291
 - Managing Change, 283-299
 - (See also Critical Success Factors)
 - Marine Corps Tactical Data Network (MCTDN), 80, 82

- Metrics, 81, 248, 272-281, 295-296
 (See also Performance Measurement)
 Service Level Agreements, 81-82, 84
- Navy Marine Corps Intranet (NMCI), 32, 61-62, 73, 80, 81-82, 84-89, 134, 138, 146, 147, 173-174, 176, 214, 225-226, 294, 301
 Action Group, 72
 Best Practices, 86
 Budget, 87
 Business Case Analysis, 86
 Information Strike Force (ISF), 81, 84, 86-88, 301
 Interoperability, 85
 Personnel, 87
 Security, 84-85
- Ontologies, 157-158
- Organizational Learning, 179, 189, 306
 (See also Learning and eLearning)
- PDA, 62-63
- People, 40, 76-77, 177-188, 203, 208, 224, 285, 291
 (See also Critical Success Factors)
- Performance Measurements, 264, 272-273, 295
 Balanced Scorecard, 273, 280, 296
 Guide for Developing and Using IT Performance Measures, 264, 266, 273, 276, 296
 KM Performance Measurement Process, 278-279
- Portal, 138, 147-151, 303
 Enterprise, 147-151, 303
- Presidential Decision Directive 63, 216, 228, 242
- Privacy, 217, 239-245
 Policy, 240-245
- Program Executive Office (IT), 61, 72, 82
- Public Key Infrastructure, 120, 163, 167, 216, 225, 303-304
- Records Management, 171-176
- Reverse Auctions, 119, 124
- Rumsfeld, Donald, Secretary of Defense, 228
- Section 508, 211-214
 Section 508 Self-Help Tool Kit, 214
- Security, 19, 78, 84-85, 215-217, 222-227
 (See Information Assurance, Critical Infrastructure Protection and Public Key Infrastructure)
- Self as an Agent of Change, 194
- September 11, 228, 243, 301-304
- Sharing, 43, 292, 304
 (See also Critical Success Factors)
- Skills, 41, 192, 195-196
 Patterning, 42, 192
 Scanning, 42, 192
 Sensing, 41, 192
- Smart Card, 110, 119-120, 163-170, 303-304
- Spectrum
 (See Electromagnetic Spectrum)
- Standards, 75-77, 97, 213, 290
 ITSG, 59, 75-77, 95, 290
- Standards and Architectures, 18
- Storytelling, 40, 42, 133
- Strategic Plan, 28, 122, 178, 247, 285
 eBusiness, 122
 Goals, 28, 30
 IM/IT, 28, 247, 249, 253, 272, 285
 Workforce, 178, 181, 186, 295
- Systems Thinking, 135-136, 189-190, 292-293

Taxonomy, 119, 138, 152-162, 293
 Definition, 153, 156
 EKMT, 152, 159-162

Technology, 30-31, 101-102, 108-111,
 113-116, 125, 128, 131, 177, 211-
 213, 224, 285-286, 294, 298-299,
 301-305
 (See also Critical Success Factors)

Technology Enablement Strategies, 108-
 116

Tools, 53-54, 93, 244, 296-297

Ubiquity, 304-305

Walker, David M., Comptroller General of
 the U.S., 301

Wearable Computers, 112, 305

Winchester Mystery House, 57

Wireless, 100, 102, 111-112, 298, 305

Workforce, 31, 36, 87, 144, 178, 180-188,
 211, 295
 IPT, 181
 Planning, 184
 Strategic Plan, 178, 181, 186, 295

Workforce Competency Management,
 178, 180-188, 295
 Career Planning Tool, 178, 295
 Civilian Career Path Guide, 295
 Continuous Learning Guidance, 184
 Inherently Governmental Guidance,
 186, 295

Y2K, 47-48, 215, 218-221

References

CHAPTER 1

United States. Cong. Clinger-Cohen Act of 1996

---. ---. Goldwater-Nichols Department of Defense Reorganization Act of 1986

---. ---. Government Information Security Reform Act of 2000

---. ---. Paperwork Reduction Act of 1995

CHAPTER 2

United States. Department of the Navy. Information Management/Information Technology Strategic Plan for 2000-2001. 2000

---. ---. Information Management/Information Technology Strategic Plan for 2002-2003. 2002.

---. ---. Information Management/Information Technology Web site. <<http://www.don-imit.navy.mil>>.

CHAPTER 3

Barquin, Ramon, Alex Bennet, and Shereen Remez, eds. Building Knowledge Management Environments for Electronic Government. Vienna, VA: Management Concepts, 2001.

Bennet, Alex. "Building the Knowledge Force of the Future: A Case Study of Knowledge Management at the Department of the Navy." Building Knowledge Management Environments for Electronic Government. Eds. Ramon Barquin, Alex Bennet, and Shereen Remez. Vienna, VA: Management Concepts, 2001. 291-311.

Bennet, Alex. "The Virtual Town Hall: Vehicle for Change." CHIPS Magazine (a Department of the Navy Publication). Fall 1999: 6-7.

Brown, John Seely and Paul Duguid. The Social Life of Information. Harvard Business School Press, 2000.

United States. Department of the Navy. Integrated Product Team Learning Campus: Gaining Acquisition Results through IPTs. Vers. 1.1a. 1998.

---. ---. Sharing e-Government Successes, Knowledge Fair 2000: Compendium of KM and eBusiness Initiatives. Vers. 1.0. 2000.

---. ---. Sharing e-Government Successes, Knowledge Fair 2001: Compendium of KM and eBusiness Initiatives. Vers. 2.0. 2001.

CHAPTER 4

- Ananthaswamy, Anil. "Tele-Immersion." GlobalTechnoScan.com. <<http://globaltechnoscan.com/25thOct-1stNov/teleim.htm>>.
- Barbian, J. "The Future Training Room." Training. Minneapolis: 38:9:40-45. Sept. 2001.
- Bass, Thomas A. "Dress Code." Wired.com. Apr. 1998.
<http://www.wired.com/wired/archive/6.04/wearables_pr.html>.
- Bell, Gordon and Jim Grey. "The Future of Computing." The Mercury News. 1997.
- Britt, Robert. "Vital Signs: Wrestling with a Wearable HAL." SPACE.com. 25 Jul. 2001.
Retrieved 25 Oct. 2001.
<http://www.space.com/business/technology/technology/jpl_devereauz010725-1.htm>.
- LaBerge, Stephen and Howard Rheingold. Exploring the World of Lucid Dreaming. New York: Ballentine Books, 1990.
- Lanier, Jaron. "Virtually There." Scientific American Magazine. Apr. 2001.
- Luciano, Elizabeth. "UMass Scientist Developing Wearable Computer That Learns: It isn't about writing a paper while you're in line at the grocery store." University of Massachusetts Amherst News Release. 5 Jan. 2000.
<<http://www.umass.edu/newsoffice/archive/2000/010500fagg.html>>.
- Nash, Jim. "Wiring the Jet Set." Wired.com. Oct. 1997.
<<http://www.wired.com/wired/archive/5.10/wiring.html>>.
- Nobel, Carmen. "Wearable computing: More than Geek Chic." eWeek. 7 May 2001.
<<http://www.eweek.com/article2/0,3959,108984,00.asp>>.
- Sanders, Jane M. "Electronic Job Performance System Provides On-the-Spot Training." Georgia Institute of Technology Press Release. 2 Apr. 1999.
<<http://www.eurekalert.org>>.
- Sherwood, Jonathan. "Give it a Thought - And Make it So." University of Rochester Press Release. 1 May 2000. <<http://www.rochester.edu/pr/releases/cs/bayliss.html>>.
- Stroud, Michael. "What's On Tap? Why Haptics." Wired.com/news. 21 Aug. 2001.
<<http://www.wired.com/news/business/0,1367,46192,00.html>>.
- United States. Department of the Navy. Architecture Development Process Model. Vers. 1.0. 2000.
- . ---. CHIPS Magazine. Special NMCI Issue. Spring 2001.
- . ---. CHIPS Magazine. Special NMCI Issue. July 2000.
- . ---. Data Management and Interoperability Implementation and Planning Guide. 2001.
- . ---. Integrated Architecture Database. Vers. 1.0. 2000.

CHAPTER 5

- Barquin, Ramon, Alex Bennet, and Shereen Remez. eds. Building Knowledge Management Environments for Electronic Government. Vienna, VA: Management Concepts, 2001.
- . ---. ---. eds. Knowledge Management: The Catalyst for eGovernment. Vienna, VA: Management Concepts, 2001.

- Bennet, Alex. "Building the Knowledge Force of the Future: A Case Study of Knowledge Management at the Department of the Navy." Building Knowledge Management Environments for Electronic Government. Eds. Ramon Barquin, Alex Bennet, and Shereen Remez. Vienna, VA: Management Concepts, 2001. 291-311.
- . "Knowledge Superiority as a Navy Way of Life." Knowledge Directions, The Journal of the Institute for Knowledge Management. Spring/Summer 2001, 46-57.
- Bloom, Benjamin S. and David R. Krathwohl. eds. Taxonomy of Educational Objectives Book I: Cognitive Domain. Longman Publishing Group, 1989.
- Brown, Mark Graham. Keeping Score: Using the Right Metrics to Drive World Class Performance. New York: Productivity Inc., 1996.
- Bukowitz, Wendi R. and Ruth L. Williams. The Knowledge Management Fieldbook. Prentice Hall, 1999.
- Davenport, Thomas H. and Laurence Prusak. Information Ecology: Mastering the Information and Knowledge Environment. New York: Oxford Univ. Press, 1997.
- Denning, Stephen. The Springboard: How Storytelling Ignites Action in Knowledge-era Organizations. Woburn, MA: Butterworth-Heinemann, 2000.
- Glass, Robert L. and Iris Vessey. "Contemporary Application-Domain Taxonomies." IEEE Software 12.4 (1995): 63-76.
- Jones, Karen Sparck. Summary Performance Comparisons TREC-2 through TREC-8. NIST Special Publication 500-246: The Eighth Text Retrieval Conference (TREC 8). 1999, U. of Cambridge. <http://trec.nist.gov/pubs/trec8/t8_proceedings.html>.
- Kaplan, Robert S. and David P. Norton. The Balanced Scorecard: Translating Strategy into Action. Boston: Harvard Business School Publishing, 1996.
- . ---. The Balanced Scorecard: Measures that Drive Performance. Harvard Business Review, Jan. 1992. 71-79.
- Liebowitz, Jay. Ed. Knowledge Management Handbook. CRC Press, 1999.
- Malafsky, Geoffrey. "Designing an Enterprise Knowledge Management Architecture." Military Engineer. May-Jun. 2001.
- Porter, Dan and Alex Bennet. "KM and eBus: A Common Focus Through Different Lenses." Chips Magazine. Fall 2000. <<http://www.chips.navy.mil>>.
- Prusak, Laurence. Knowledge in Organizations. Philadelphia: Butterworth-Heinemann, 1997.
- Rademacher, R.A. "Applying Bloom's Taxonomy of Cognition to Knowledge Management Systems." Proceedings 1999 ACM SIGCPR Conference on Computer Personnel Research. New Orleans.
- Ranganathan, S.R. Prolegomena to Library Classification. 2nd ed. Library Association, London. 1957.
- Sacco, G. M. "Dynamic taxonomies: a model for large information bases." IEEE Transactions in Knowledge and Data Engineering. 12: 468. 2000.
- Senge, Peter. The Fifth Discipline: The Art and Practice of the Learning Organization. New York: Currency/Doubleday, 1990.
- Snowden, D. "The Paradox of Story: Simplicity and Complexity in Strategy." Journal of Strategy and Scenario Planning. Nov. 1999.
- Stewart, Thomas A. Intellectual Capital: The New Wealth of Organizations. New York: Doubleday, 1997.
- Sveiby, Karl Erik. The New Organizational Wealth: Managing and Measuring Knowledge-

- Based Assets. San Francisco: Berrett-Koehler Publishers, 1997.
- Taulbee, O.E. "Classification in Information Storage and Retrieval." Proceedings ACM National Conference. 1965.
- United States. Department of the Navy. Knowledge-Centric Organization Toolkit. Vers. 2.0. 2001.
- . Federal CIO Council. Knowledge Management Working Group CD.
- . Government Accounting Office. Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investment. Mar. 1998.
<<http://www.gao.gov>>.
- Vasconcelos, Jose. et al. "A Group Memory System for Corporate Knowledge Management: An Ontological Approach." Proceedings of 1st European Conference Knowledge Management. Sept. 2000.
- Wiegand, Wayne A. and Donald G. Davis. Eds. Encyclopedia of Library History. New York: Garland Publishing, 1994.
- Wiig, Karl M. Knowledge Management Foundations: Thinking About Thinking - How People and Organizations Represent, Create and Use Knowledge. Texas: Schema Press, 1994.

CHAPTER 6

- Bennet, Alex. "Knowledge Management: Unlocking the Potential of Our Intellectual Capital." CHIPS Magazine. Winter 2000. <<http://www.chips.navy.mil>>.
- Eisenberg, Michael B. and Doug Johnson. "Computer Skills for Information Problem-Solving: Learning and Teaching Technology in Context." ERIC Digest. Mar. 1996.
- Edvinsson, Leif and Michael S. Malone. Intellectual Capital: Realizing Your Company's True Value by Finding it's Hidden Brainpower. New York: Harper Business, 1997.
- Goodridge, Elisabeth. "Feds Turn to eLearning to Cut Costs." Information Week Magazine. 4 Jun. 2001.
- National Academy of Public Administration. News Release. Civilian Workforce 2020: Strategies for Modernizing Human Resources Management in the Department of the Navy. Washington, DC. 2001. <<http://www.napawash.org>>.
- . ---. The Transforming Power of Information Technology-Making the Federal Government an Employer of Choice for IT Employees. Washington, DC. 2001.
<<http://www.napawash.org>>.
- United States. Comptroller General. "Human Capital - Building the Information Technology Workforce to Achieve Results." Testimony before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, U.S. House of Representatives. 2001.
- . Department of the Navy. C-port: Building Communities of Practice. Creating Value through Knowledge Communities, Practitioner's Guide. Vers. 1.0. 2001.
- . ---. Knowledge Superiority Conference. U.S. Naval Academy. Annapolis, Maryland. 1999.
- . ---. Naval Personnel Task Force. A Strategic Human Resource Management System for the 21st Century. Volume I. Oct. 2000.
- . ---. ---. A Strategic Human Resource Management System for the 21st Century.

- Volume II. May 2001.
- Wenger, Etienne. Communities of Practice: Learning, Meaning, and Identity. Cambridge, Mass: Cambridge University Press. 1999.
- . Supporting Communities of Practice: A Survey of Community-Oriented Technologies. <<http://www.km.gov>> under "Group Documents," then "Documents and Resources." 2001.

CHAPTER 7

- United States. Department of Defense. Critical Infrastructure Protection (CIP) Plan: A Plan In Response to Presidential Decision Directive 63 "Critical Infrastructure Protection." 18 Nov. 1998.
- . ---. Critical Infrastructure Protection Integration Staff Implementation Plan. March 2000.
- . ---. Critical Infrastructure Protection Integration Staff Implementation Plan. May 2001.
- . Department of the Navy. Chief Information Officer. Initiatives for Full Dimensional Protection.
- . ---. Critical Infrastructure Protection Implementation Plan. 1 Jul. 2002.
- . ---. 26 Aug. 1999. Memorandum. DON Critical Infrastructure Protection.
- . ---. Secretary of the Navy Instruction 3501.1. Department of the Navy Critical Infrastructure Protection. 16 Jun. 2002.
- . Senate. Judiciary Committee. Know the Rules, Use the Tools, Privacy in the Digital Age: A Resource for Internet Users. <<http://judiciary.senate.gov/oldsite/privacy.pdf>>.

CHAPTER 8

- Malhotra, Yogesh. "Knowledge Management for E-Business Performance: Advancing Information Strategy to Internet Time." Information Strategy: The Executive's Journal. 16.4 (Summer 2000): 5-16.
- Martinsons, Maris, Robert Davidson, and Dennis Tse. "The Balanced Scorecard: A Foundation for the Strategic Management of Information Systems." Decision Support Systems. 25 (1999) 71.
- United States. Department of the Navy. Chief Information Officer. Blanket Purchase Agreement Best Practices. 2001.
- . ---. ---. Guide for Developing and Using IT Performance Measurements. Vers. 1.0. 2001.
- . ---. ---. IT Investment Portfolio Management Model. 1999.
- . ---. ---. IT Investment Portfolio Management Guide. 2002.
- . ---. ---. Metrics Guide for Knowledge Management Initiatives. 2001.

CHAPTER 9

- Bennet, Alex. "Managing Change in a Knowledge Environment." Knowledge Management: The Catalyst for Electronic Government. Eds. Barquin, Ramon, Alex Bennet, and Shereen Remez. Vienna, VA: Management Concepts, 2001. 335-360.
- Bennet, Alex and David Bennet. "Characterizing the Next Generation Knowledge Organization." Knowledge and Innovation: Journal of the KMCI. 1.1 (2000): 8-42.
- ,---. "Exploring Key Relationships in the Next Generation Knowledge Organization." Knowledge and Innovation: Journal of the KMCI. 1.2 (2001): 91-108.
- Conger, Jay Alden, Gretchen M. Spreitzer, and Edward E. Lawler. eds. The Leader's Change Handbook: An Essential Guide to Setting Direction and Taking Action. San Francisco: Josey-Bass, 1999.
- Edelman, Gerald M. and Giulio Tononi. A Universe of Consciousness: How Matter Becomes Imagination. New York: NY: Basic Books. 2001.
- Emig, Janet A. Web of Meaning: Essays on Writing, Teaching, Learning, and Thinking. New Jersey: Boynton/Cook Publishers, Inc. 1983.
- Espejo, Raul, Werner Schuhmann, Markus Schwaninger, and Ubaldo Bilello. Organizational Transformation and Learning: A Cybernetic Approach to Management. New York: John Wiley & Son Ltd., 1996.
- Griffith, Samuel B. Introduction. The Art of War. By Sun Tzu. Oxford University Press. 39. 1963.
- Kotter, John P. Leading Change. Boston, MA: Harvard Business School Press, 1996.
- Senge, Peter. The Fifth Discipline: The Art and Practice of the Learning Organization. New York: Currency/Doubleday, 1990.
- United States. Department of the Navy. C-port: Building Communities of Practice. Creating Value through Knowledge Communities, Practitioner's Guide. CD-ROM. Vers. 1.0. 2001.
- , ---. Information Literacy Toolkit CD. Vers. 1.0. 2001.
- , ---. Information Management/Information Technology Strategic Plan for 2000-2001. 2000.
- ,---. Knowledge-Centric Organization Toolkit. CD-ROM. Vers. 2.0. 2001.
- ---. Learning in a Virtual World CD. Vers. 1.0. 2002.
- ,---. Systems Thinking: A Language for Learning and Action. CD-ROM. Vers. 2.0. 2001.
- ,---. Workforce Competency and Career Planning. CD-ROM. 2001.
- ,---. Chief Information Officer. "Building the Knowledge Enterprise." KM Presentations. 2000 and 2001.
- ,---,---. Metrics Guide for Knowledge Management Initiatives. 2001.

CHAPTER 10

- Barbian, J. "The Future Training Room." Training. Minneapolis: 38:9:40-45. Sept. 2001.
- Bass, Thomas A. "Dress Code." Wired.com. Apr. 1998.
 <http://www.wired.com/wired/archive/6.04/wearables_pr.html>.
- Bell, Gordon and Jim Grey. "The Future of Computing." The Mercury News. 1997.
- Britt, Robert. "Vital Signs: Wrestling with a Wearable HAL." SPACE.com. 25 Jul. 2001.

- Retrieved 25 Oct. 2001.
<http://www.space.com/business/technology/technology/jpl_devereauz010725-1.htm>.
- Forbes. "E-Learning: Building Competitive Advantage Through People and Technology." Retrieved 28 Nov. 2001. <http://www.forbes.com/special_sections/eLearning/e-02.htm#a>.
- Lanier, Jaron. "Virtually There. Three-dimensional tele-immersion may eventually bring the world to your desk." Scientific American. April 2001.
<<http://www.scientificamerican.com>>.
- Luciano, Elizabeth. "UMass Scientist Developing Wearable Computer That Learns: It isn't about writing a paper while you're in line at the grocery store." University of Massachusetts Amherst News Release. 5 Jan. 2000.
<<http://www.umass.edu/newsoffice/archive/2000/010500fagg.html>>.
- Advisor. "What Trends are Shaping E-Learning?" Retrieved 26 Nov. 2001.
<<http://www.advisor.com/Articles.nsf/aid/SMITT187>>.
- Sanders, Jane M. "Electronic Job Performance System Provides On-the-Spot Training." Georgia Institute of Technology Press Release. 2 Apr. 1999.
<<http://www.eurekalert.org>>.
- Shachtman, Noah. "New Army Soldiers: Game Gamers." Wirednews. 29 Oct. 2001.
<<http://www.wired.com/news/conflict/0,2100,47931,00.html>>.